Co-working spaces are the new trend nowadays. They provide flexible and comfortable environment to digital nomads and entrepreneurs. However, the very fact that a coworking space is shared environment for people with different backgrounds means that it comes with potential data security risks. All it needs is one malicious member to infiltrate into the system and compromise the data of all others. This is why, it is crucial to establish a secure and strong network for your co-working space to keep all digital information safe and safeguard your customer data and devices from being hacked. At the same time, coworkers themselves need to think of several things to keep their data secure.

Let us look at security from both sides, as a coworking space provider and as a coworker.

Below are some important measures you need to take to enhance and ensure the security in your coworking space.

**Securing your Co-working Space as a Provider**

**Create an Access Control Policy**

Invest and install a reliable access control solution which guarantees satisfaction to the members and also attracts new members. Whether the solution is based on smart cards, biometrics or access code based, it must contain entire information of each individual user. A cloud-based access control solution is even better, as its access log will allow you to track who goes where and when in your coworking space. You can also allow full-time access or put a time-limit, and put access restriction to designated areas or certain meeting rooms within your space.

**Ensure Physical Security**

It’s an unfortunate fact that things get lost or stolen even in the best communities. To prevent this, you need to ensure that the equipment of coworking members stays secure.

To [protect yourself against equipment theft](https://www.homesecurityheroes.com/), the easiest and most obvious step is to install surveillance cameras in and outside your workspace. Outdoor cameras should ideally be waterproof, infrared for night vision, give full view, and have motion detection enabled for non-working hours. Install a cloud-based camera to monitor real-time access to your office even when you are away from the location.

Provide secure desks to coworkers where they can safely lock and secure their important documents or equipment while they are away.

Since coworking spaces attract many visitors, it is imperative to guide them seamlessly throughout your space. A random guest walking aimlessly in your premises does not give good vibes. Provide visitor badges to distinguish them from regular members and also keep a log record of all visitors that visit your space.

Last but not the least, protect your space against the risk of fire. Install a fire alarm system to get immediately alerted if there is even slightest sign of fire.

**Ensure Network Security**

Once you have enabled access control and physical security, make sure that all your networks are password-protected and separated from your main network. Also, to prevent previous members from accessing your network, change passwords and SSIDS of your WIFI devices frequently. You can also consider using a mesh network with AP controllers which can help you manage IPs and devices with access to WIFIs. It can also allow you to monitor bandwidth of devices and blacklist any unwanted devices on the network. An electric timer to shut down WiFi access overnight is also a good investment for security.

**Hire Responsible Front Desk Staff**

The front desk staff that is in charge of greeting visitors can make or break the company’s impression. For coworking spaces, however, it is not only a matter of good impression, but also being able to handle visitor safety and security. It is important that they are well trained and understand the importance of security for your coworking space and its members. When your front desk staff prioritizes branding and security needs and can provide input on improving the check-in process from these perspectives, you have a valuable asset in your hand.

**Securing Your Coworking Space as a User**

Whether you are a freelancer, entrepreneur, or work-from-home professional, you need to keep your equipment and valuable data secure for personal or professional reasons. Even with a coworking space that provides complete security, you still need to be vigilant about any threats lurking around your confidential information. Leaving your laptop or documents unattended even for a short time may allow another person to steal your information. Make sure to lock all your valuables in the desk space provided by the facility. Always install and update anti-virus and firewalls in your system, and ask the front desk to verify from you whenever any person visits as your guest.

Though security is often overlooked, it is vital to prioritize it and apply preventive measures to make sure that your space and community stays safe.