A Resolution for Corporate Network

To handle the hackers around the world. Please use Desktop or Laptop without WIFI Function, use traditional "ETHERNET CARD" for network connection instead. Let say for instance in the Banking Industry. Each teller or counter's PC is connected with "RJ45" cables to the "ETHERNET CARD". I assume and suppose the PCs of the teller at the counter will not be able to access outside **INTERNET** world. They will not be able to browse website. As I said, close area network is the **UTIMATE** solution. You create your own small Bank area network, without accessing outside. Programs development, emails, documents, storages.... can be access only inside your enterprise. You can still use ROUTERS and SWITHCES and all those networking methods, the main point is you are not allow to access or be accessed from the outside world!! This kind of network has a term call “**Intranet**”. You may argue you need to have network connection for overseas countries! Yes, as I said minimize the chance of being Hack. You can use “**Proxy Server**” to connect to overseas countries, That means you have a large close area network that span across 2 countries, with each has a close area network.

This kind of close area network has several advantages: First you are focusing on your job, without disturb by the outside internet world. I assume you should not be watching TIKTOK during program development. Second you will not be able to download unlicensed software. But program development needs packages or software in order for development. Yes! so that is why enterprise has their own software repository (licensed software, authorized freeware...), that needs to be approved and checked by it’s own IT department. Without worrying employees violating copywrite rules and also downloading malware softwares. If the employees needs to access outside world to look for information. They can bring their own laptop or perhaps provide one for them which allows them to access outside world, but the main point is it should be seperated from the corporate network, and also these laptops or PCs are strictly not allowed to connect to the enterprise internal network. The corporate may have strict rules or regulations which they are not allowed to have "ETHERNET CARD" installed on their personal laptop or PCs, they are only allowed to use **WIFI** for network connection. **USB** or other external devices are not allowed to use. So, all the corporate PCs or laptops does not have **USB**, **DISC driver** installed. How about work from home? as I said, minimized the chance of being hacked. The only way is you can only use the corporate provided PCs or Laptops for taking home. This Laptops or PCs provided by the corporate has installed Enterprise Grade Security Software and has complicated connection method which allows you to connect to the corporate internal system. Close area network also provides several advantages, such as less malware or viruses, because you are not accessing the outside world, internal emails or emails received from outside are being internal scan, so the chance of being malware or virus affected will greatly be reduce. Also **reducing** the costs of installing large complicated anti-virus systems to monitor your corporate laptops and PCs. The only disadvantages is you should have a naming standard or IP numbering standard for each laptop or PCs inside the corporate. Several large network can be grouped as several small sub area network. As you are creating your own internal network, you are not consuming the outside world IP addresses, whiich benefits of public IP not enough issue.