# Roving Users and Shared Workstations: Security Challenges

## What is a Shared Workstation?

Shared workstations are corporate business trends that are commonly used in workplaces with staff that work during different shifts throughout the day. A common example of a shared workstation is a hospital. Hospitals operate 24/7, but each nurse works approximately 40 hours a week. Therefore, hospitals establish day and night shifts where some nurses work during the day and then swap with the nurses working during the night. Because day-shift nurses and night-shift nurses work at different times, their schedules do not collide, and they can work at the same desk. Other known examples such as libraries and call centers operate in a similar manner. They are all large contributors to the growth of shared workstations.

## Roving Users

Employees who work through shared workstations have been coined the term, "roving users". Roving users refer to the service model where employees will constantly be on the move instead of being stationed at one location. Common cases of roving users are librarians and nurses because during their shift, they will be continuously on the move. For one, librarians will be continuously move around the building, restocking returned books, maintaining the quiet environment of the library, and helping customers finding the book that they want.

Similarly, roving users also symbolize that employees will never be stationed at the same desk as call centers where employees are assigned to use a different cubicle every shift.

### Pros

There are benefits to having a shared workstation:

- Works best in small officers with frequent verbal communication.
- There is no need for emails, phones, or walking to other desks. There is easier collaboration and networking.
- It creates friendliness and camaraderie.
- It saves space and money on office product expenses, so two employees can share the same stapler, phone, and computer.

### Cons

There are also detriments to having a shared workstation:

- With unnecessary conversation and interaction, employees might not complete projects and assignments on time.
- There is little privacy among the employees, and there are security issues.
- There is a lot of noise pollution, and plenty of distractions because even though everyone has light and heavy days, not everyone will have them at the same time.
- Personal belongings could be missing.

## Shared Accounts

As aforementioned, shared workstations allow two or more employees to work at one computer. Therefore, instead of having two or more computers per employee, the one computer will have as many accounts as necessary. Shared Accounts are self-explanatory; they are accounts that are shared among the employees, and there are different types of shared accounts.

For one, libraries setup anonymous and guest accounts for visitors to log in to the system and use a computer. These accounts have access to an external server to download files or programs, and there is no password required. However, anonymous and guest accounts are big risks for a company. Although guest accounts have limited access to the server compared to an administrator, they allow *anyone* into the system, and this is risky because the default access for most guest accounts allows them to access data that they should not have access to view.

For two, any company may set up temporary employee accounts for employees that will be with the company temporarily. Generally titled, “temp_1”, these accounts are set up so that the temporary employee has access to the server once they are in the office. The largest risk with temporary employee accounts is that the new employee will have access when they should not. If a salesman goes on vacation, a temporary employee will fill in and have access to the files that the vacated salesman has including past records, downloaded files, etc.

For three, companies must establish administrator accounts which are accounts shared among all higher-up employees and IT professionals when necessary. These administrator accounts have access to the entire server and have no limitations. They can access all the accounts and the files on those accounts as well as create new accounts and change the configuration settings. If a new employee joins the staff, the administrator account can add their information into the system and set them up with a password. There are large risks with the administration accounts because these accounts can corrupt data within the system or even delete the information from other administrators.

# Shared Workstations Security Practices

Because the largest number of risks is based on the access of the Domain Administration Group, there are plenty of security practices that protect the system and the company.

Primarily, there should be no day-to-day access to Administration accounts. Only higher-ups and administrators within the company should have access to the Administration accounts when necessary, but general employees should not have access. The problem is that it is gotten easier for attackers to obtain user credentials through keystroke logging and pass-the-hash. When an attacker has access to a general employee’s account, they plan to move laterally within the network to obtain access to the Administration account.

Secondarily, companies should use two types of accounts: an account with minimal permissions to get the job done and an administrative account. Imagine a salesman within the company who has administrative access has a very simple password. An attacker through keystroke logging discovers his user credentials, and logs into the account. Because the salesman has administrative access, the attacker now has administrative access meaning company-wide access to any file within the entire system. However, if the salesman only had general access, the attacker only has access to his files, and can only perform minimal and limited damage.

Lastly, companies should do anything that they can to secure the administrative account. Even though passwords are out-of-date, passphrases and biometric technology have played a large part in protecting the administrative account.

# Biometrics and Roving Workers - Shared Workstations

Roving workers are common in banks as tellers move from one station to another, or as supervisors authorize transactions. Roving workers are also common in warehouse environments. It’s tempting for employees to share passwords or be exposed to the password of a colleague. Biometric authentication eliminates the risk and temptation associated with password sharing or stealing. Additionally, the static free one-touch authentication enabled by ones biometric, compliments workflow and delivers the best user and customer experience.

Shared workstations, common in call centers and shared POS systems, common in retail also present high-security risks. Users in these environments are often part-time employees that are associated with high turnover and a minimal commitment to the organization, thus increasing the threat of theft or rogue behavior. Transactions can be fast paced in these environments opening the door for short-cuts and risk to the overall process. Biometric authentication eliminates the need for swipe / ID cards in retail, which are vulnerable to sharing and easily lost or misplaced – adding to the cost of operations.  In call centers where agents work in close quarters, it’s relatively easy to see a fellow agent enter their password.  By nature, call centers have many agents, which only increases the risk of password fraud.  When call centers add biometric sign-in they positively identify the agent using something the “are” rather than a random password.  Biometric sign-in is ideal for crowded – fast-paced work environments.

References:

https://activedirectorypro.com/active-directory-security-best-practices

https://douron.com/shared-workstations-benefits/

https://www.allbusiness.com/are-shared-workstations-a-good-idea-4113418-1.html

https://www.rocketspace.com/tech-startups/what-are-the-pros-cons-of-shared-office-space

https://www.sans.org/reading-room/whitepapers/basics/paper/1271