SECURITY-MINDED

Practical security wisdom for daily life.

KEEP IT CLEAN

Simple 'clean desk' habits can improve workplace security

When it comes to your personal workstation, do you prefer obsessive organization or cheerful clutter? Some suggest that a messy or tidy desk affects a person's creativity, efficiency, and focus. But you might be surprised to learn how much your workspace habits can affect your organization's security.

Leaving devices unlocked or sensitive information out in the open—on desks, screens, and other work areas—increases the risks of theft, data breaches, and other threats.

Many organizations have employees follow a clean desk policy (CDP). This policy typically explains how to secure information and clear workspaces at the end of the day. Even if you don't have a CDP (or the requirements are minimal), developing "clean desk" habits is an easy way to improve security.

Why Does a Clean Desk Matter?

First, think about all of the people who could walk by your desk or work area. Here are a few common examples:

- Cleaning crews
- Building management
- Maintenance personnel
- Construction workers
- Vendors
- Service providers

That's a lot of strangers! Some of these people may have access while you're away, such as as during evenings, weekends, and holidays. Others could plausibly walking by your desk at almost any time. Even a private office with a locked door could be accessed by others for legitimate purposes.

Now, with these people in mind, take a moment to think about:

- What they might see on your unlocked screen or papers left out on your desk (including passwords*)
- What they'd find if they rummaged in an unlocked drawer
- What would happen if they stole your unattended device or credentials

*See next page, "Sticky-Note Syndrome"

Criminals, Coworkers, and the Curious

If your organization is being targeted, a criminal might try to access your workspace. Clever scammers use social engineering tactics to trick people into giving them access to a building or a secure area. An intruder might impersonate an employee, vendor, or service provider, for example.

But an outsider doesn't have to be malicious to compromise security. A vendor or service provider could post seemingly harmless details about their workday online—maybe a photo of an especially cluttered desk! Their actions could inadvertently expose your sensitive information.

Who could access your desk while you're away—and what would they find?

STICKY-NOTE SYNDROME

A security mistake that's all too common in the workplace is to keep passwords handy by writing them down on sticky notes or a piece of paper. *Writing down your passwords is extremely unsafe*, whether they're stuck to your monitor, hidden under your mouse pad, or placed in an unlocked desk drawer.

Anyone walking by could quickly steal it or snap a photo. A cyber criminal could use your stolen credentials to access sensitive information and systems, resulting in serious consequences.

If you need help with managing your passwords safely, ask your IT or information security team for advice.

Another crucial group to consider: your coworkers. In your job, you may handle sensitive information that your coworkers should not see. Imagine that an HR staff member leaves documents on their desk that reveal an employee's salary or private information. Compromising that person's privacy and security could create risks for individuals and the organization.

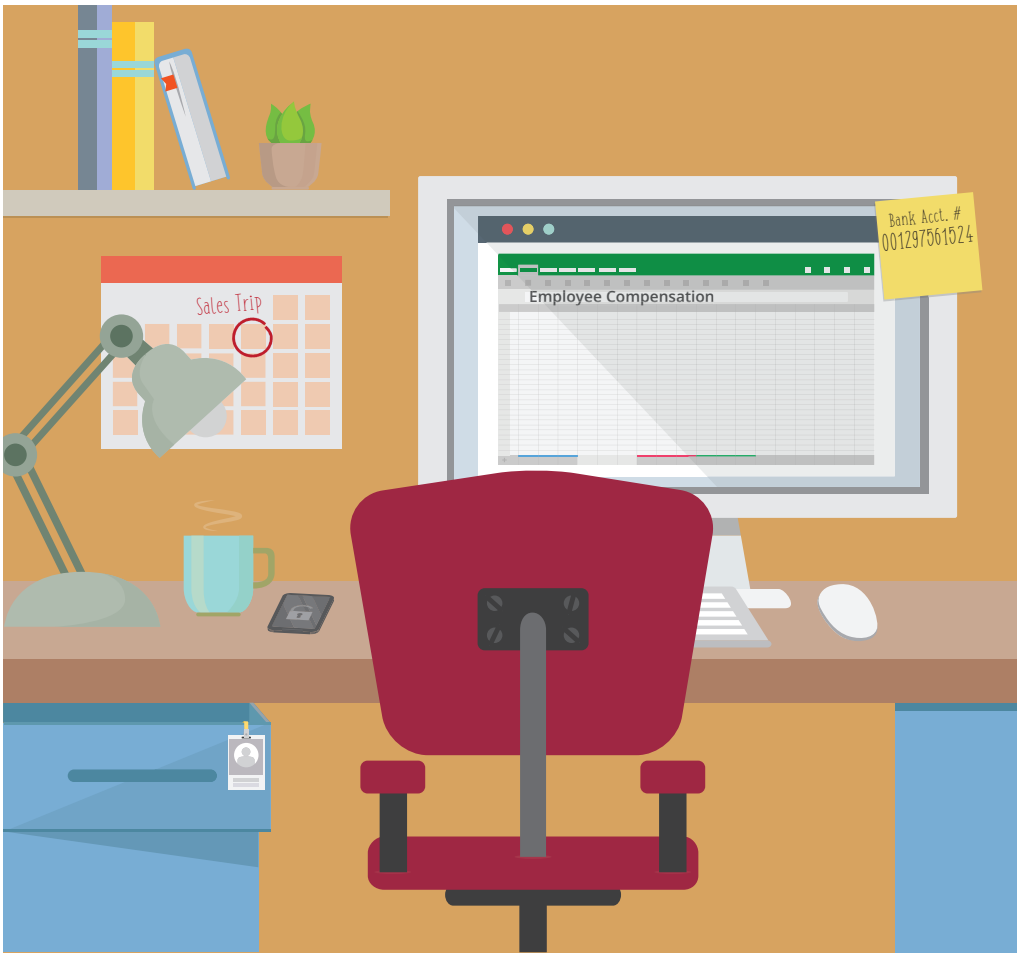
What Can I Do?

Follow these clean desk tips to help keep your workplace secure:

- **Computers and Screens –** Any time you leave your desk (even for just a few minutes), lock your computer to protect it from unauthorized access and prying eyes.
- **Mobile Devices –** Whenever possible, carry smartphones, tablets, and other small devices with you. Otherwise, lock them in a drawer or cabinet.
- **Sensitive Information –** Secure sensitive files and data at all times. Don't leave passwords, folders, calendars, planning notes, or portable storage media exposed.
- **Keys and Badges –** Always keep your keys, access cards, or fobs with you. Or, secure them in a desk drawer or cabinet, per your organization's policies.
- **Final Check –** Before leaving for the day, power down your devices and lock up any portable electronics you are leaving behind (laptops, tablets, smartphones, etc.).

Activity Corner // What's Wrong With This Picture?

Find the five risky security habits in this workspace.



Answers:
1. Calendar with work trip visible
2. Mobile device unlocked
3. Bank account number on sticky note
4. Desk drawer open
5. Private excel doc open