SECURITY-MINDED
Practical security wisdom for daily life.

# PHYSICAL SECURITY FACTS

## Protecting against thieves, intruders, and other attacks

Throughout history, people have used physical security measures to ward off attacks—from castle gates to gated communities, from ancient walled cities to today's home security systems. Organizations also need to protect their data, facilities, and other assets from physical threats. These threats can include theft and other malicious attacks—even careless employee behavior.

### What Is Physical Security?

Think about any security measures you encounter at work. How many locked doors do you have to pass through to get to your workstation? Do you pass guards and cameras? Here are some common types of physical security:

- **Barriers and Controlled Access** – Fences, gates, and security guards are examples of barriers. Requiring an ID badge or key fob to enter are examples of access controls designed to prevent unauthorized entry.
- **Surveillance** – Security cameras help deter intruders, theft, and other malicious activity. Cameras may watch important areas such as records rooms, loading docks, and point-of-sale machines.
- **Secured Data and Assets** – Locked file cabinets help deter theft and unauthorized access. Similarly, servers and other valuable equipment may be stored in secured rooms.

### Guarding the Gates

You also play a critical role in physical security, which starts with keeping scammers out. Scammers may try to trick you into letting them into a building or secure area, using a variety of techniques. Tailgating, for example, is when an individual follows another person through a secure entrance without providing their own credentials.

To prevent tailgating, be cautious about holding the door for visitors—including delivery people. Always close doors securely behind you. Since scammers may impersonate legitimate visitors to gain access, accompany visitors to reception or the security desk. When entering with coworkers, ask them to scan their badges or key fobs so that the organization has an accurate record.

Similarly, be wary if you get an email or phone call from a stranger requesting access to the building or other resources. The person could be a scammer. Even if the request seems legitimate, verify it first with a *separate* phone call or email.

If you see something suspicious, report it. For example, if you notice an unlocked drawer or an open door that should be locked, it could mean that sensitive data was accessed. An unauthorized person or an

If you see something suspicious, report it.

unaccompanied visitor in a restricted area could indicate a physical security breach.

## What Can I Do?

- **Keys, Badges, and Fobs** – Keep these items with you to prevent someone else from accessing buildings or systems.
- **Devices** – Always lock your computer when you walk away from your workstation. Immediately report unauthorized use of your computer or the loss or theft of a device.
- **Whiteboards** – Make sure unauthorized people can't see whiteboards. Erase sensitive information after meetings and at the end of the day.
- **Sensitive Documents** – If you aren't actively using them, secure any physical files that contain business, employee, or customer data. Collect printouts or faxes that contain sensitive data right away.
- **Server or Record Rooms** – Keep these rooms locked to protect valuable systems or data from unauthorized people.

You can learn more about physical security in your organization's security awareness training.

## Activity Corner // What's in Your Workplace?

To complete this quiz, take a walk around your workplace and put a check mark next to each item you notice. Add up the points to reveal the level of physical security at your organization.

### 1 point

□ Desk littered with potential confidential information
□ Calendar on display with important meeting dates
□ Suspicious USB drive

### 5 points

□ Confidential files stored in an unlocked filing cabinet
□ Unattended mobile device
□ Forgotten key fob or ID badge

### 10 points

□ Login credentials written on a sticky note
□ Whiteboard displaying past meeting notes
□ Unlocked computer

### -5 points

□ Privacy protectors on screens
□ An employee who scans their badge despite walking in with a group
□ Documents properly shredded before disposal
□ Security cameras

| | |
|---|---|
| **< 0** = Place of Protection | **1-5 points** = Center for Concern |
| **6-10 points** = Dangerous Digs | **11 <** = Exposed Environment |

**Final Score:**

## HELPING FAMILY AND FRIENDS STAY SAFE

**Physical security is always important, whether you are at work, at home, or traveling. Here's some good advice to share with family and friends:**

1. **Don't leave devices unattended** – Laptops, tablets, and phones are easy to steal. Keep them with you whenever possible. Use strong PINs and passwords on your devices to help protect data in case of theft.
2. **Stay aware of your surroundings** – If you're having a conversation or talking on the phone, look around: Could someone overhear personal or confidential information?
3. **Stop shoulder surfers** – "Shoulder surfers" try to watch what you type or see your screen. Shield your screen from others before you enter a PIN or password and avoid accessing sensitive information in public.