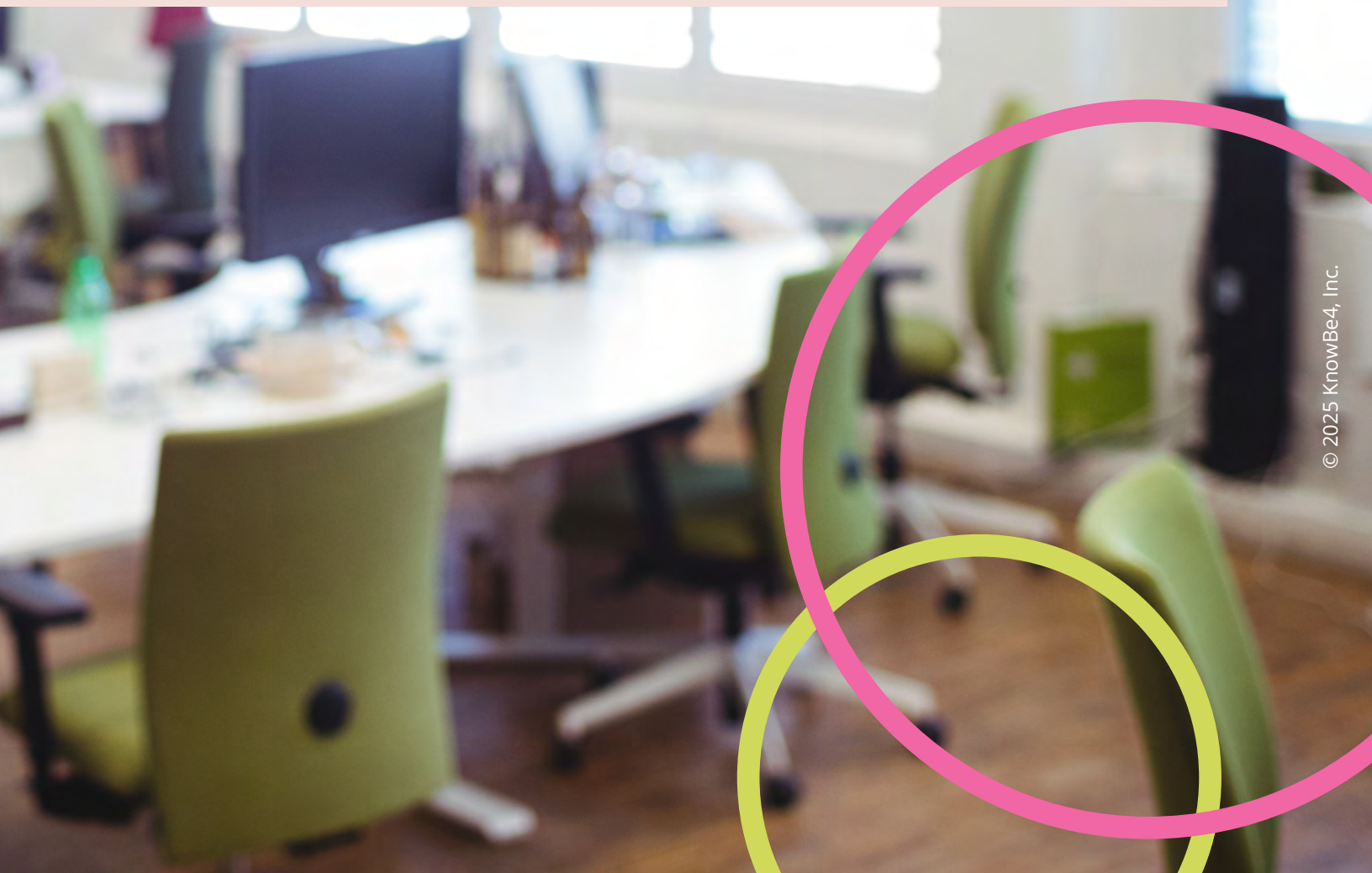
SecurityAwarenessNews
the security awareness newsletter for security aware people

SECURING THE PHYSICAL DOMAIN

Preventing Unauthorized Access
Securing Your Work Environment
Nontechnical Security Basics



© 2025 KnowBe4, Inc.

PREVENTING UNAUTHORIZED ACCESS

THE SILENT ENTRY

An organization employee holds the door open for someone carrying boxes, not realizing this person doesn't have authorized access to the building. This common courtesy, while well-intentioned, could lead to a serious security breach.

WHAT IS UNAUTHORIZED ACCESS?

Unauthorized access occurs when individuals gain entry to restricted areas without proper credentials or permission. It's one of the most common physical security threats, often happening through simple methods like **tailgating** (following closely behind an authorized person to slip through a secure door) or **social engineering** (using manipulation and deception to trick people into granting access) rather than forced entry.

WHY IT MATTERS

While cybersecurity often takes center stage, physical security breaches can be equally devastating. An unauthorized person with physical access can:

- Steal sensitive documents or equipment
- Plant malicious devices
- Access restricted network points
- Compromise employee safety

RECOGNIZING COMMON ENTRY TACTICS

Tailgating and social engineering are not the only methods of physical security threats. Stay alert for these other frequent unauthorized access methods:

STOLEN CREDENTIALS: Using lost or stolen access cards

DOOR PROPPING: Keeping secure doors unlocked for convenience

© 2025 KnowBe4, Inc.

SECURING YOUR WORK ENVIRONMENT

Physical security isn't just about locks and cameras — it's about maintaining awareness and following proper procedures consistently. Every employee plays a crucial part in maintaining physical security.

ACCESS CONTROL BEST PRACTICES

- Always wear your ID badge visibly
- Never loan your access card to others
- Report lost credentials immediately
- Verify visitors follow proper check-in procedures

SECURE SPACE MANAGEMENT

- Keep sensitive documents locked away
- Lock your computer when stepping away
- Secure all doors and windows properly
- Make sure that no sensitive documents, notes, or devices are left on your desk when you leave

© 2025 KnowBe4, Inc.

NONTECHNICAL SECURITY BASICS

The most effective physical security measures often don't require complex technology — just consistent attention to basic principles. Here are some essential security habits:

MAINTAIN AWARENESS

- Be aware of your surroundings
- Know who belongs in your work area
- Question unfamiliar faces politely
- Trust your instincts if something seems wrong

FOLLOW PROTOCOLS

- Use designated entry points only
- Sign visitors in and out properly
- Keep emergency exits clear
- Know and follow evacuation procedures

REPORT ISSUES

- Report suspicious activities promptly
- Document security incidents
- Alert maintenance about facility issues
- Share security concerns with supervisors

© 2025 KnowBe4, Inc.

Physical security isn't just the responsibility of your security team — it's a shared commitment. Every time you properly display your badge, question a tailgater, or secure your workspace, you're actively protecting your organization. While some actions like displaying the badge, questioning a tailgater, or securing your workspace might seem small, they create a strong security culture that helps keep everyone safe.