5 PHYSICAL SECURITY BEST PRACTICES

Being aware, informed, and engaged can make all the difference.

Sometimes relatively low-tech defenses can be just as important as sophisticated antivirus and network security software. This is certainly the case with physical security measures.

Elements like locks, passwords, physical barriers, and surveillance systems are key components in an organization's overall security portfolio. But like any element of security, the human factor plays a significant role. Employees who are aware, informed, and engaged can make all the difference.

In order to ensure you are not a weak spot in your organization's physical security, follow these best practices:

1. **Ensure all locks reengage**
Double check that secure doors close completely and that you relock any cabinets, drawers, closets, or safes that hold sensitive materials. Make sure that keys are not left in locks or in view.

2. **Keep important items secure**
If you are stepping away from your desk, lock your computer, take your ID badge and mobile phone, and lock up any files or devices that contain sensitive information. And be sure not to share important personal items like passwords, security codes, access tokens, and ID badges.

3. **Destroy unwanted data**
Don't throw away or recycle confidential files and CDs, shred them. If you are retiring hardware, including USB devices, check with your IT department about eliminating old data so it cannot be recovered and used.

4. **Eliminate unauthorized access** You should not hold or open secure doors for people you don't know, and you should not grant access to secure areas to anyone who doesn't have confirmed authorization. Make sure people are who they say they are, and ensure that strangers don't sneak in a secure door behind you when you enter.

5. **Travel smart**
When you are outside the office, keep your devices and confidential materials safe. Your car is not a secure storage option, not even the trunk. If you can't keep items with you, opt for a hotel safe or a secure cabinet or closet with limited access. If you're overseas, then carry devices with you when possible, to be extra secure.

6. **Bottom Line: Be Aware**
It's important to understand and use physical security best practices because you are part of your organization's defense against breaches. Don't be afraid to ask questions if you see something out of the ordinary. And if you suspect a breach has happened, report it to your manager and your security department as soon as possible. Quick action can help minimize damage.

proofpoint

CYBERSECURITY HEROES