Physical Security

An organization's employees are one of the biggest risks to its cybersecurity. In fact, human error is considered the leading cause of data breaches.

However, security awareness isn't just about what resides on your company's computers or handheld devices. Be aware of potential security risks in physical aspects of your workplace as well.

Follow These Best Practices to Help Ensure the Safety of Physical Data on Your Devices and Your Workspace

Shoulder surfing

Be aware of people watching as you type -do not allow others to stand over you and watch your keystrokes (known as "shoulder surfing")

Watch out for "impersonators"

Don't let in visitors claiming to be inspectors, exterminators or other vendors without verification.
Ensure they have proper identification and a scheduled appointment.

This card is to admit entrance to the employee pictured ONLY. Do NOT allow anyone else in with you.

No tailgating allowed!

Secure entrance protocols are there for a reason - do not allow someone to follow you through a door into a restricted area (called "tailgating")

If it's broken, fix it!

Do not ignore malfunctioning physical security controls such as doors, locks, fingerprint or card readers. Immediately notify security and maintenance personel to get the issue resolved.

Don't make your passwords public

Passwords are not protected if you leave them written on paper on your desk, in a drawer, or under your keyboard or desk mat!

Password protect your computer

Password protection is essential to ensure others don't get unauthorized access to data - it only takes a few seconds to access information. Lock or Logoff your computer whenever you are not present.

Do not leave your devices in plain sight

Keep your phones, tablets, and laptops out of view. Leaving them on your desk or in an open purse or briefcase puts you at risk for it being accessed or stolen.

Institute a Clean Desk Policy

Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. A clean desk policy should state that information visible on a desk should be limited to what is currently necessary. Before leaving the workspace for any reason, all sensitive and confidential information should be securely stored.

Need Help Securing Your Business?
Contact Anjolen Inc:
Michelle Tuttle: mtuttle@anjolen.com