SecurityAwarenessNews

the security awareness newsletter for security aware people

THE THREATS AMONG US

EXTERNAL THREATS
PHYSICAL THREATS
INSIDER THREATS

EXTERNAL THREATS

One of the most important functions of security is identifying and circumventing external threats — those that come from outside an organization. These threats manifest themselves in a number of ways and typically involve cybercriminals who have a variety of motives. Here's how they attack organizations and people:

PHISHING

As always, phishing represents the top attack method for many cybercriminals. Phishing emails often contain malicious links or attachments designed to steal confidential information. Attackers will also phish people via phone calls, text messages, and other forms of communication.

MALWARE INFECTIONS

One of the biggest threats to security is malware, which is malicious software that infects devices. Ransomware is a prime example of malware. It encrypts data or locks systems to prevent organizations from accessing valuable resources until they pay a ransom to the attackers.

SOCIAL ENGINEERING

Social engineering refers to the manipulative techniques attackers use to scam people. Most scams feature some form of social engineering by pushing a sense of urgency, using threatening language, or offering fraudulent promises of financial gain.

These are only a few examples of external threats and the dangers they present. You can avoid them through a combination of awareness and patience. Slow down and think before taking action. Stay alert for common warning signs of scams, and don't assume someone is who they claim to be.

As always, people represent the last line of defense when it comes to maintaining security and privacy. Thanks for doing your part!

PHYSICAL THREATS

While online threats tend to garner the most attention in the world of security, physical threats pose just as much risk.

TAILGATING

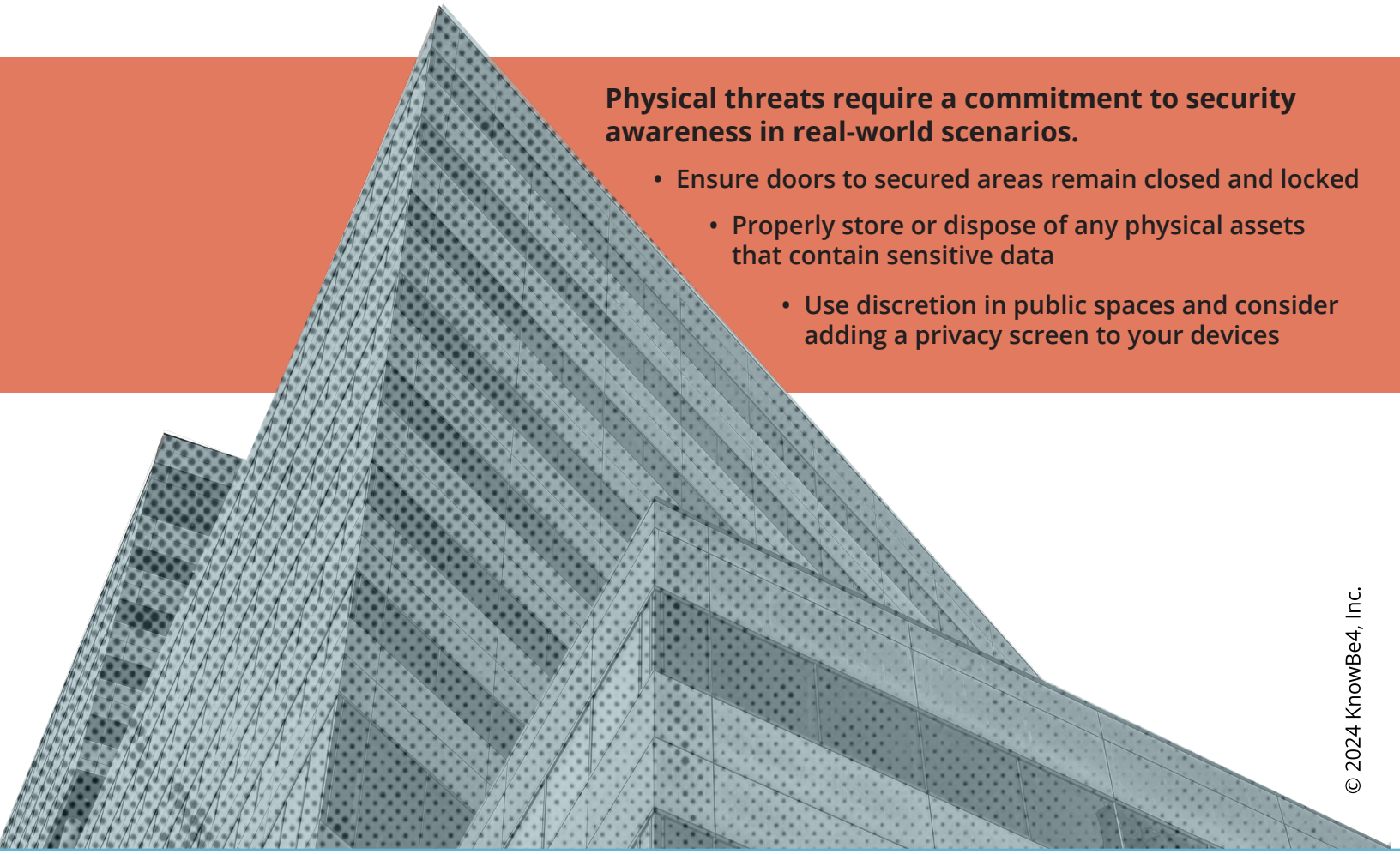
Physical access to buildings and workplaces offers a lot of value to criminals. That's why they might attempt to sneak in behind someone after that person unlocks a door — an attack known as tailgating. As unlikely as that scenario sounds, it remains a possibility and is a firm reminder to utilize situational awareness.

DEVICE THEFT

Lost or stolen laptops, smartphones, and tablets are not only costly to replace, they also put confidential data at risk. Some thieves will attempt to extract any information they can from a stolen device before selling it to someone else.

DUMPSTER DIVING

Some scammers have no shame in digging through trash or recycle bins. Their hope is to find confidential documents or discarded smart devices where the data hasn't been properly erased. Dumpster diving is one of the oldest tricks in the book and it requires no technical skills.



Physical threats require a commitment to security awareness in real-world scenarios.

- Ensure doors to secured areas remain closed and locked
- Properly store or dispose of any physical assets that contain sensitive data
- Use discretion in public spaces and consider adding a privacy screen to your devices

INSIDER THREATS

An insider is anyone with some level of physical or digital access to an organization. Insiders can include employees, business associates, contractors, and others. An insider threat is when any part of that chain knowingly or unknowingly creates security incidents or undermines an organization's core values.

Insider threats fall into three categories: malicious, negligent, and accidental. Let's review each one in a little more detail.

MALICIOUS

Malicious insiders abuse access to intentionally cause harm to their organizations. Why would anyone want to do this? It could be a disgruntled employee who is unhappy in their work environment. It could also be someone who steals proprietary information or sells trade secrets to competitors for financial gain.

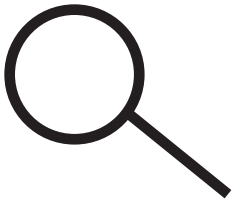
NEGLIGENT

Most insider threats don't have malicious intentions. In fact, a lot of threats are created by someone making a decision that might violate policy or cause unnecessary risk to security. Using weak or repeated passwords is a simple example. Leaving a work-issued device where it can be easily stolen is another example.

ACCIDENTAL

People make mistakes. Unfortunately, human error is one of the leading causes of security incidents. Examples of those mistakes can include:

- Opening a malicious link or attachment
- Sending confidential information to the wrong person
- Misplacing a work device or ID badge



As an insider, you can help maintain security and privacy by:

- **Always following organizational policies**
- **Reporting anything suspicious immediately**
- **Using strong, unique passwords for every account and device**