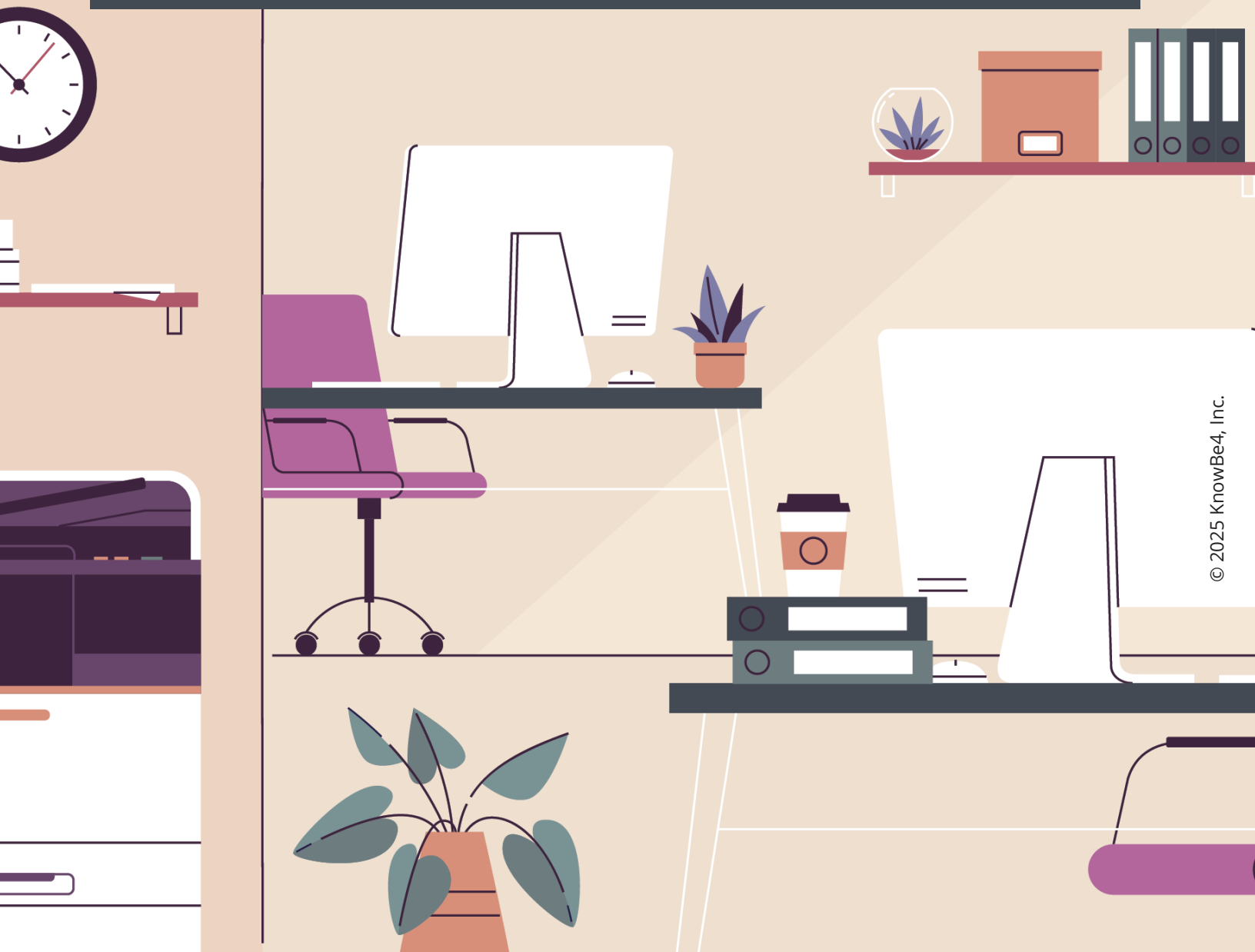
SecurityAwarenessNews
the security awareness newsletter for security aware people

Zero Trust Security

Never Trust; Always Verify
Situational Awareness
People, Processes, and Technology



Never Trust; Always Verify

Traditional security models trusted users inside network perimeters. This worked when applications were on-premises and most employees worked in offices. Today's landscape of cloud services, remote work, and personal devices has dissolved boundaries, making default trust a significant vulnerability.

An email appearing to come from inside the organization network might automatically pass traditional security filters. An employee could receive a message from their "CEO" requesting an urgent fund transfer and, with no security flags raised, proceed with the transaction — an attack that additional verification steps in a Zero Trust model would likely prevent.

Zero Trust is a security approach requiring all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated before accessing applications and data. The core philosophy is simple: "Never trust; always verify." It is founded on three key principles:

Verify explicitly:

Authenticate using multiple data points, including user identity, device health, and location.

Use least privilege:

Provide only the access needed for specific tasks through just-in-time permissions.

Assume breach:

Segment networks, limit access scope, encrypt data, and continuously monitor for threats.

These principles, combined with end-user security awareness, create a robust, in-depth strategy that helps keep people, assets, and data safe.

Situational Awareness

Situational awareness — being mindful of your surroundings and potential security threats — is essential to Zero Trust security. While technology implements verification controls, your active awareness detects threats that technical measures might miss.

For example, imagine receiving a phone call from someone claiming to be from IT about an urgent security issue. They need you to provide your username and password so they can install a vital security update. In this scenario, your awareness should kick into Zero Trust mode and remind you that it's never a good idea to provide your passwords to anyone for any reason.

That's the core idea behind situational awareness. It's taking a moment in any given scenario to process what's happening to determine the legitimacy of requests (especially when money or confidential data are involved). This also includes physical security, such as staying alert for unknown individuals attempting to access secured areas.

Situational awareness is a simple way of putting Zero Trust into action by approaching each interaction with thoughtful questions: Is this person really who they're claiming to be? Why would they need this information right now? Is this how we normally handle this type of scenario? What's the best way to verify if this situation is legitimate?

Remember, your awareness is an invaluable security tool that complements technical defenses. If you notice anything suspicious, be sure to report it immediately.

People, Processes, and Technology

Successfully implementing Zero Trust security isn't just about having the right tools. It's about creating a proper balance between three essential components: people, processes, and technology. Let's review all three to better understand what they mean.

People: The Decision Makers

People represent the last line of defense and one of the most important parts of the security chain. In a Zero Trust environment, everyone plays a crucial role in maintaining security and privacy.

Your security responsibilities include verifying before sharing any information, promptly reporting security concerns, and actively participating in security training.

Processes: The Guide

Without clearly defined processes, even the most security-conscious people and sophisticated technology can't create a robust, secure environment. Conversely, well-designed processes provide the structure that makes security consistent and effective.

The Zero Trust approach relies on processes like regular identity verification, access management procedures, and many other components based on the needs of the organization. The goal is to create detailed security strategies for handling various threats with a well-documented incident response plan.

Technology: The Technical Foundation

Technology provides the tools needed to implement Zero Trust principles at scale without sacrificing productivity. While these tools will vary from one workplace to another, they often include comprehensive endpoint security solutions, encryption, and network segmentation to contain potential threats.

This pillar also involves ensuring that these tools are implemented correctly and that systems and software stay updated. Outdated systems could allow attackers to infiltrate an organization unnoticed.

A Complete Framework

From handling requests for information or money to creating security policies and maintaining technology, everyone plays a vital role in an organization's security efforts. You can continue doing your part by staying alert for threats, following policy, and never assuming someone is who they claim to be.