May 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people

Gatekeepers: The Guardians of Data

People, Processes, and Technology
The Gatekeeper's Playbook
Being the Last Line of Defense at Home

© 2023 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

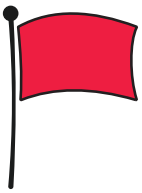
PEOPLE, PROCESSES, AND TECHNOLOGY

Ensuring confidential information remains confidential requires an overlap of three key areas: people, processes, and technology. In fact, those elements represent the foundation of a framework that has existed since the 1960s — a model designed to help organizations assess and improve performance.

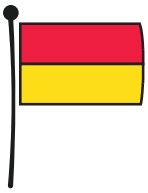
The idea behind the framework is that all three overlapping components must be aligned and properly balanced for an organization to achieve and maintain a successful workflow.

Not long after it was introduced, the framework was adopted by the security community. To this day, it is one of the most widely used for information technology management as well as workforce management.

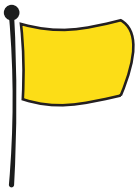
It's also a perfect model for cybersecurity and the effort every organization makes to defend data. Let's review each component and what they mean for you.



PEOPLE - These are the individuals at every level of an organization who must make smart decisions, protect the access they've been granted, and maintain security through their actions. Even though the "people" element is considered the first pillar of the framework, people are also the last line of defense when it comes to identifying and mitigating cyberthreats.



PROCESSES - These are the procedures and policies that define how things are done. They include how passwords should be created, which personal devices employees are allowed to connect to networks, and how to report security incidents. It's your responsibility to understand what those policies require and follow them at all times.



TECHNOLOGY - These are the systems, hardware, and software that support people and processes. While most employees have no control over the technologies an organization uses, they do have control over how they use that technology. Simple examples include locking workstations when not in use, storing portable devices securely, and never bypassing any security controls.

The people, processes, and technology framework provides a simple way to understand how the three most crucial components of an organization work together to achieve a common goal: protecting data, systems and, more importantly, people.

© 2023 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

THE GATEKEEPER'S PLAYBOOK

In a literal sense, the term gatekeeper refers to someone who monitors and controls entry points to buildings or properties. It's a concept that's as old as time but still applies to modern-day work environments, particularly where security is concerned.

In that regard, gatekeepers are the individuals who control access to people, data, and systems. They're equipped with the know-how to identify threats and maintain a security-first mindset that reduces mistakes that endanger data privacy. Here are five strategies every gatekeeper needs in their playbook:

FOLLOWING POLICY

Policies are designed to prevent data leaks and maintain the security of employees, clients, customers, and business associates. Your commitment to following those policies eliminates unnecessary risk and keeps everyone's private information safe.

USING COMMON SENSE

If something sounds off, if it's too good to be true, or if any scenario seems far-fetched, then react accordingly. When you have doubts, don't ignore them. Follow your instincts and never assume someone is who they say they are.

THINKING BEFORE YOU CLICK

Phishing attacks attempt to mislead people by creating fraudulent scenarios intended to steal data or money. You can spot these attacks by looking out for common warning signs such as urgent or threatening language, poor grammar, or unexpected links or attachments.

MAKING A PERSONAL PLEDGE

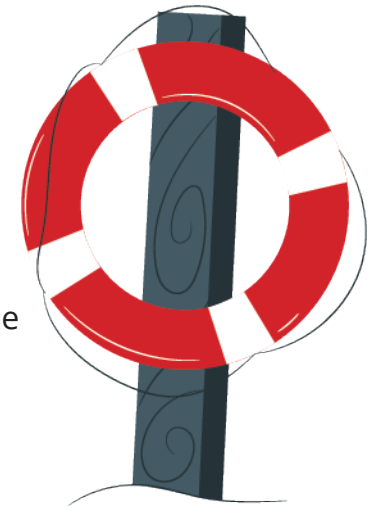
By making a pledge to view security as a personal matter, you enter a mindset that recognizes confidential information as the representation of someone's livelihood. Remember, we all have personal information that gets collected by a large number of organizations. Thus, we all have something to lose when security efforts fail.

REPORTING INCIDENTS IMMEDIATELY

A security incident includes any event that could lead to unauthorized access to data, systems, or members of an organization. In a perfect world, security incidents would never occur, but the growing cyber landscape offers a different reality. By reporting incidents immediately, you help reduce the damage they could cause.

© 2023 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

BEING THE LAST LINE OF DEFENSE AT HOME



Every organization owes it to their employees, customers, and business associates to ensure sensitive information remains protected. That's why security awareness programs carry so much importance. Similarly, you owe it to yourself and your household to use the awareness gained through those programs to protect yourself and your loved ones.

After all, you are the last line of defense. Your actions and decisions determine your digital safety, regardless of which devices or software you use. Reinforce personal security by using these defensive measures:

PROTECT YOUR INBOX

One of the biggest mistakes anyone can make is assuming that phishing attacks are reserved for large organizations. Cybercriminals will gladly enter anyone's inbox, hoping to spread computer infections or steal confidential data. As always, stay alert and keep an eye out for common warning signs, just like you do at work.

THINK LIKE A SCAMMER

Scammers often create fictitious scenarios to gain and exploit trust. You can identify these situations by thinking about it from their perspective. How would you convince someone to send you money or sensitive information? Use that line of questioning when dealing with those requests and allow skepticism to guide your thought process.

UPDATE DEVICES

Outdated devices and software provide cybercriminals an opportunity to exploit security vulnerabilities. These vulnerabilities are commonly posted in public forums when discovered. That's why manufacturers and developers routinely issue updates to patch crucial security flaws. Enable automatic updates so you never miss an important fix.

UTILIZE SECURITY TOOLS

While there's no such thing as a flawless security tool, there are many options you can utilize to upgrade your security. Examples include:

- **Antivirus software** identifies and removes malicious programs
- **Ad-blocker** reduces potentially dangerous pop-ups
- **Multi-factor authentication** requires more than one password to access accounts

PRIORITIZE ONLINE PRIVACY

One of the keys cybercriminals need to unlock their scams is your personal information. They find those keys by creating social media profiles in search of any details you've made public. Prioritize your online safety by setting your social media accounts to private, vetting all friend requests, and limiting the amount of personal information you share.

© 2023 The Security Awareness Company - KnowBe4, Inc. All rights reserved.