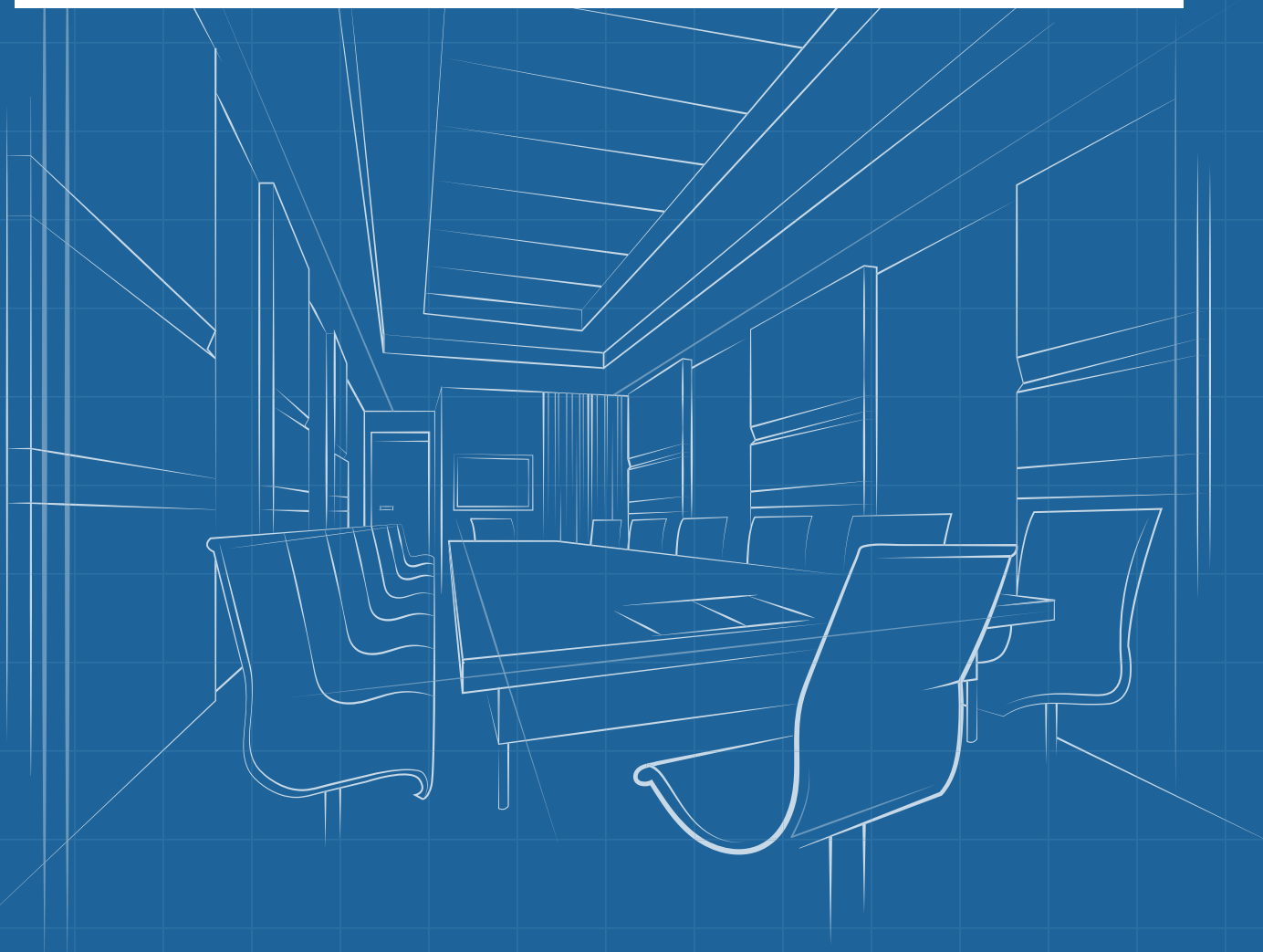
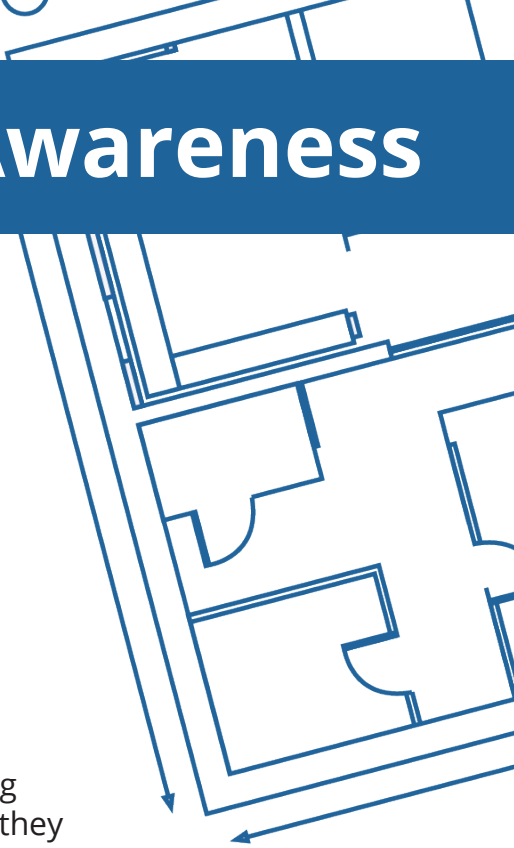
SecurityAwarenessNews
the security awareness newsletter for security aware people

Security by Design

Mastering Situational Awareness
Strong Password Hygiene
Why Policy Matters



Mastering Situational Awareness



In the world of technology, "Security by Design" refers to building systems that prioritize security as a core function, rather than adding it as an afterthought. You can also use that principle in your day-to-day routines by viewing security as a fundamental responsibility, regardless of your role or location.

Situational awareness is a key part of that process. It's a proactive approach to identifying potential threats before they can materialize. Here's what it means in practice:

Staying Alert for Warning Signs

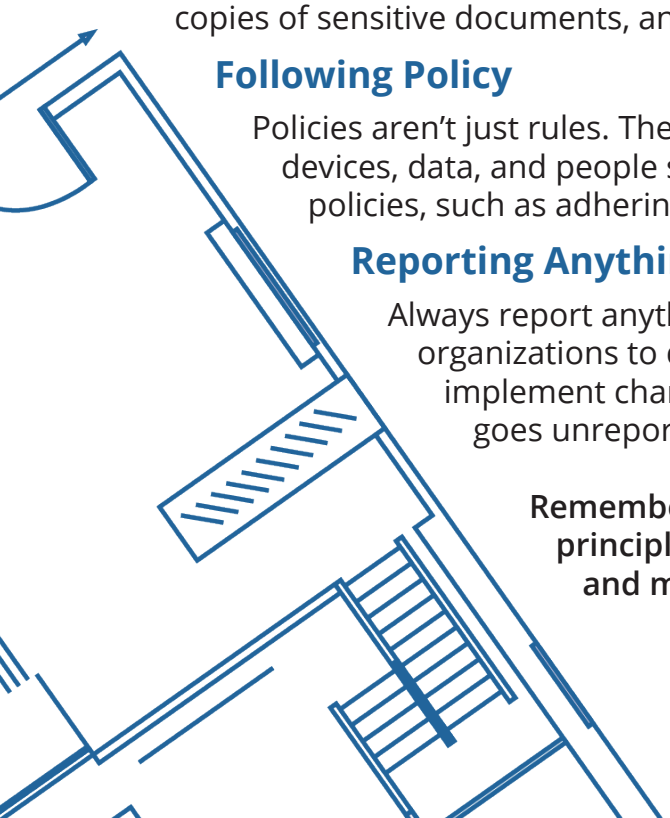
Attackers often attempt to bypass security controls by manipulating human emotions. Meaning, they don't hack devices or computers; they hack humans. Stay alert for common warning signs of this, such as threatening language, urgent requests, and unexpected links or attachments.

Remaining Skeptical

If something seems off, or if a request from IT or leadership feels out of character, don't just comply; verify it. Use a secondary communication method (like a quick in-person chat or a phone call) to confirm the request is legitimate. Never assume someone is who they claim to be.

Remembering Physical Security

Physical security is about controlling the perimeter of your workspace, regardless of where you work. Examples of this include locking workstations when not in use, securely storing physical copies of sensitive documents, and maintaining an organized workspace.



Following Policy

Policies aren't just rules. They are a part of Security by Design efforts that aim to keep devices, data, and people safe. You can do your part by consistently following these policies, such as adhering to approved workflows and using authorized tools.

Reporting Anything Unusual

Always report anything suspicious immediately. Timely reporting enables organizations to quickly review what happened, minimize damages, and implement changes to prevent future incidents. The longer an incident goes unreported, the greater the potential harm it may cause.

Remember, you are a vital line of defense. By applying the principles of Security by Design, you can help neutralize threats and maintain a safe and secure work environment.

Strong Password Hygiene

Who are you? Can you prove it? That's the basics of logging into an account or device. You provide your username and password, and the system lets you in.

But password security is complex and predates the internet. Long before the first computer booted up, ancient Roman soldiers used spoken passphrases to guard their camps at night. They also had to ensure their adversaries never figured out those passphrases, because for as long as people have had secrets to protect, others have been trying to steal them.

Today, many centuries later, you face the same dilemma as the Roman soldiers. Your digital life is locked behind these modern-day secrets. And just like in ancient times, attackers are always trying to steal those secrets.

This makes passwords a fundamental part of security. Even so, many people overlook this vital concept. Some individuals choose weak passwords that are easily guessed. Others might use the same password for multiple accounts, putting all of them at risk should that password be stolen or leaked. And to complicate matters, there's no single agreed-upon password standard.

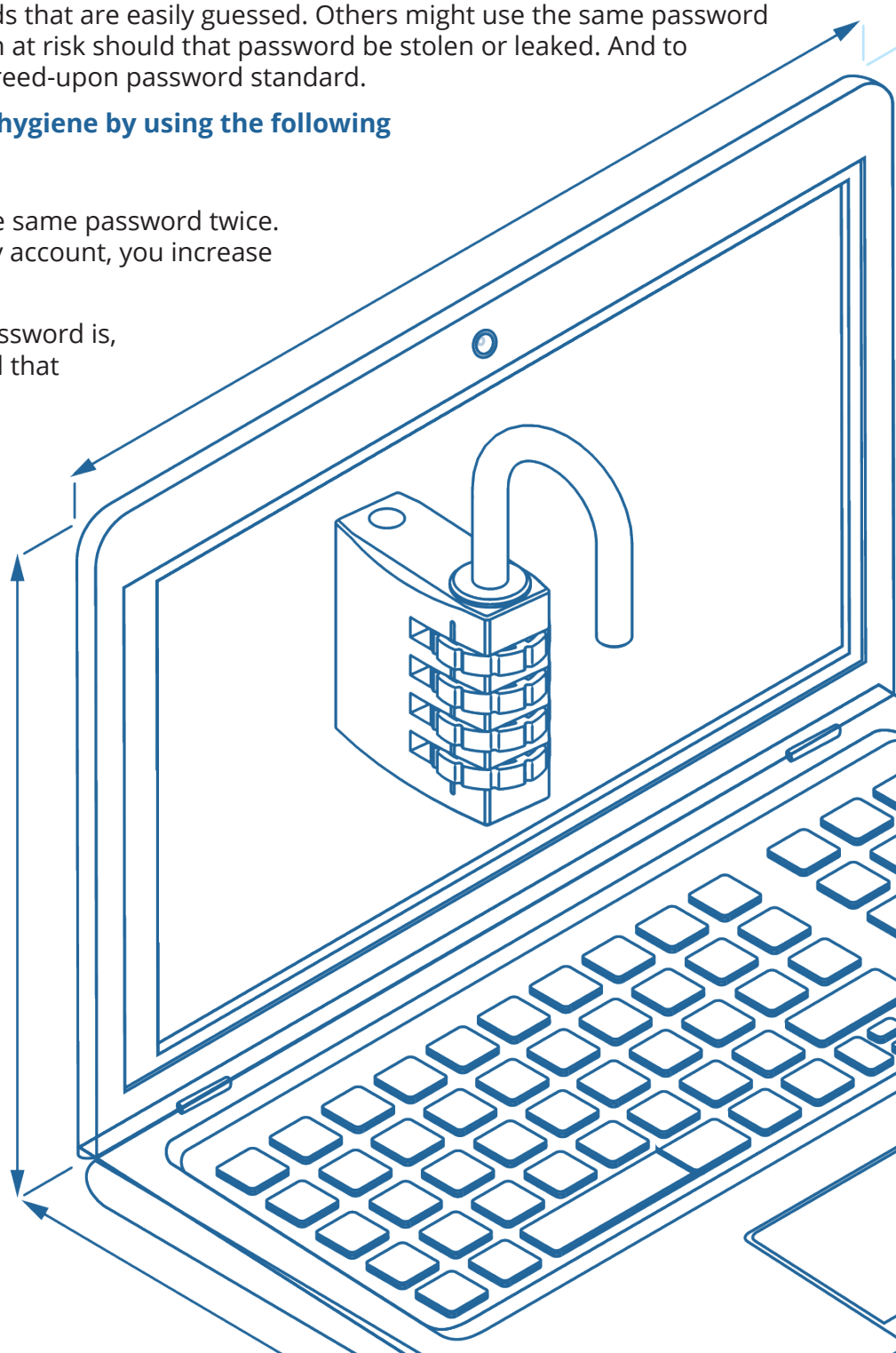
Still, you can improve your password hygiene by using the following recommendations:

Make them unique: Never use the same password twice. By creating unique versions for every account, you increase your overall security.

Prioritize length: The shorter a password is, the easier it is to guess. Keep in mind that attackers can use password-hacking tools that can automatically crack passwords, especially when they're short.

Enable multi-factor authentication (MFA): MFA is a security tool that requires at least two forms of authentication before granting access to an account. Enable it everywhere it's available.

Use a password manager: A password manager is software that can create, store, and sync all of your usernames and passwords. You only need to remember one main password to unlock the software.



At work, always adhere to your organization's password guidelines. This includes how long passwords should be, when they should be changed, and whether you're allowed to use a password manager.

Why Policy Matters

Sometimes, redundancy is a good thing. That's the case for a concept you've probably encountered repeatedly: always following organizational policies.

These customized sets of guidelines are vital to making security a default part of daily operations. To get a better idea of what that means, let's review five reasons why policies are so important.

One: Policies help organizations manage risk.

Policies exist to help establish which data privacy regulations must be followed, how data is classified, who gets access to that data, and for how long. Without policies, organizations could not overcome the challenges of identifying the what, when, where, why, and who of information security.

Two: Policies proactively prevent incidents.

Security incidents happen. They happen less often when policies are in place (and followed). For example, many organizations prohibit team members from installing random applications. If that policy isn't in place, it could result in someone downloading malicious software that steals data.

Three: Policies keep people safe.

While cybersecurity is always a top priority, physical safety is equally important. Policies play a crucial role in keeping people safe in emergency situations, extreme weather events, and other threatening circumstances. They're also a vital part of reducing workplace abuse and harassment.

Four: Policies raise overall awareness.

From password creation procedures to incident response to physical access controls, policies do more than simply build a set of rules for everyone to follow. They help raise awareness of how to reduce risk and avoid mistakes that lead to unwanted consequences.

Five: Policies lead to success.

There's an old saying that goes, "If you fail to plan, you are planning to fail." It refers to the idea that preparation is a key part of success. This is why most organizations create policies, such as incident response plans, which provide clear guidelines for handling incidents, including cyberattacks.

Remember, circumventing policies, whether intentionally or unintentionally, can put the entire organization at risk. Conversely, always following policies is one of the easiest ways to protect data, devices, and people.