SecurityAwarenessNews

the security awareness newsletter for security aware people

Access Control and You

The Basics of Access Control

Preventing Unauthorized Access

Taking Access Control Home

The Basics of Access Control

Access control determines how members of an organization may use or access resources within a computer system, network, or physical environment. It combines policies and technologies that manage and monitor access at various levels.

Why is access control important? Think about it like this:

- ***Should someone who works in sales have access to every employee's personal details, like salary information?***
- ***Should someone who works in customer support have access to high-level business strategies?***
- ***Should someone who works in marketing have access to IT administration accounts?***

The answer in all cases is no, and the idea here is clear: Access control is intentional. Every member of an organization needs only enough access to do their jobs effectively. This is known as the principle of least privilege. It's an important concept that enables organizations to control who has clearance to do what and why.

In short, your role and job function will determine what you get access to, both physically and digitally. Sometimes, security concepts are that simple. The reasoning is also simple. Imagine if a cybercriminal hacked the account of a salesperson. If that person had access to every employee's personal information, the attacker would now have access to all that information.

Access control policies are designed, in part, so security incidents like that won't grow into a much bigger problem. While implementing these measures is the job of security teams or management, protecting access is everyone's responsibility, regardless of their roles. You can do your part by:

- ***Using strong, unique passwords for every account***
- ***Never sharing your credentials, like passwords or badges, with anyone***
- ***Always following organizational policies***

Preventing Unauthorized Access

Here's the thing about access: you have it; cybercriminals and scammers want it.

They want to access networks or systems to steal confidential data. They want to hack someone's email account so they can send requests for wire transfers. They want to gain physical access to buildings and devices.

Don't let them get what they want. Prevent unauthorized access by putting these action items into practice.

Enable Multi-Factor Authentication (MFA)

MFA is a security feature that requires at least two forms of authentication before access is granted. The key benefit of MFA is that even if attackers steal a password, they're less likely to have access to additional authentication factors. Therefore, the account or system in question will block their access.

Mind Your Surroundings

When you enter secured areas, make sure no one slips in behind you. Don't let others use your ID or badge for any reason, and ensure doors remain locked and secured. If you work remotely or travel, always keep an eye on your belongings so they won't be misplaced or stolen.

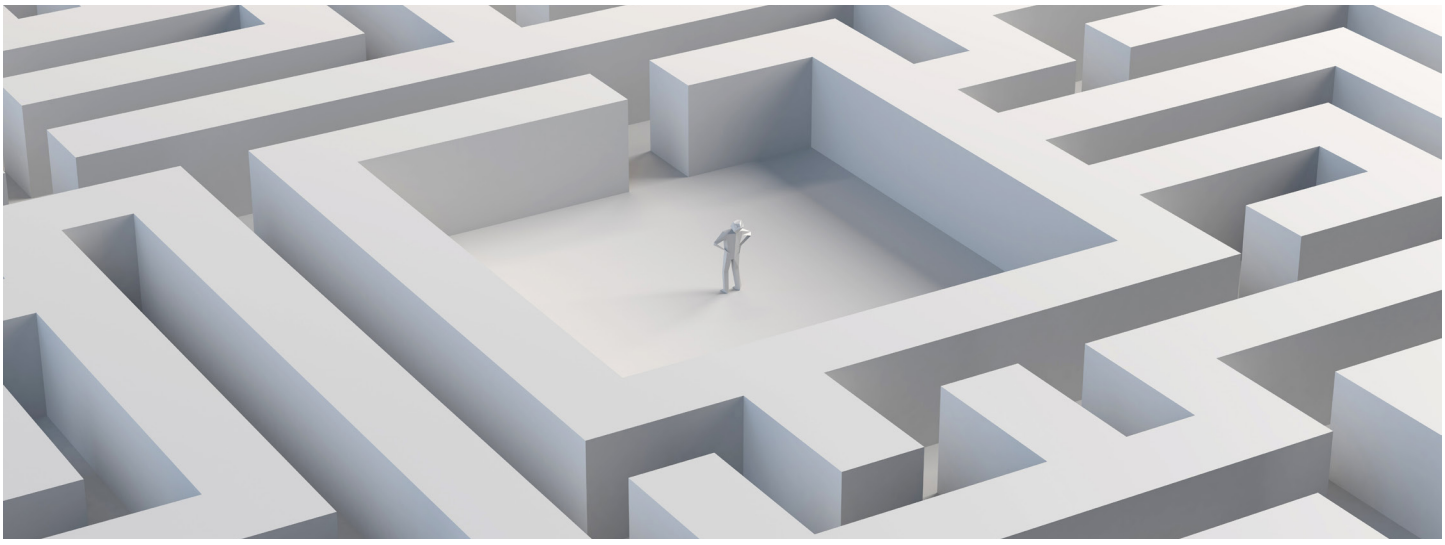
Lock Devices

Locking workstations and devices may not sound like a big deal, but it is a simple yet vital part of security. Locking a computer takes mere seconds and can be done with the stroke of a few keys. Set up mobile devices to lock after a few seconds of inactivity or, more ideally, lock them immediately when not in use.

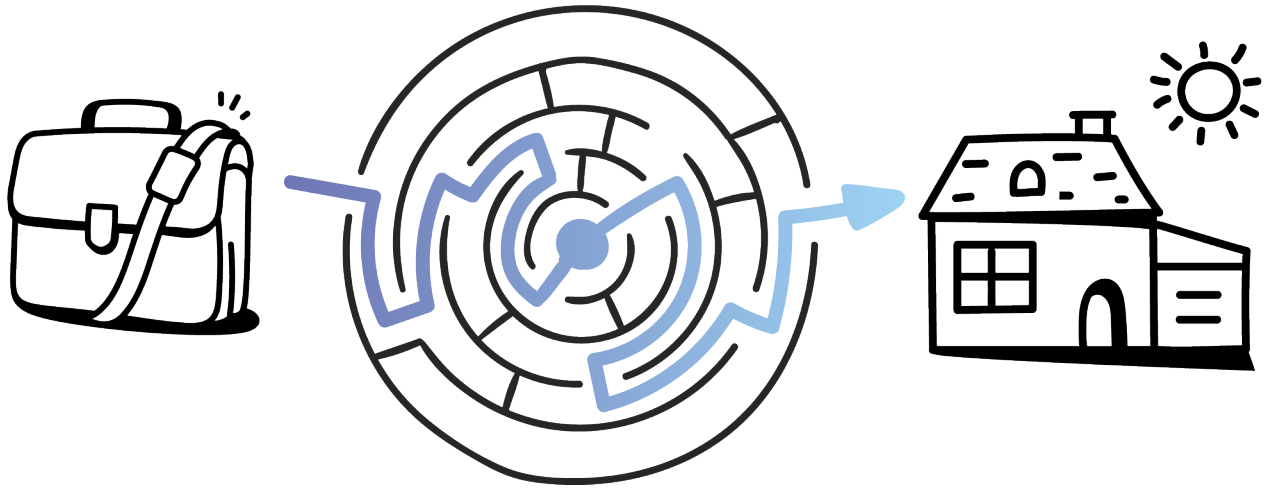
Stay Alert for Scams

Scammers use various methods to defraud people and organizations of money or information. Stay alert for the usual warning signs of their tactics, which include threatening language, urgent requests, unexpected links or attachments, and unrealistic promises.

Be sure to report anything suspicious immediately. Doing so empowers your organization to investigate the incident and mitigate any potential damages.



Taking Access Control Home



Access control policies are crucial for organizations to prevent unauthorized access to data, systems, and people. Those policies can just as effectively be applied at home to enhance the security and privacy of your household. Here are a few ways to make this concept personal:

Separate User Accounts

If you have a shared computer or device, it's wise to set up separate user accounts and assign one person as the administrator. Administrators can modify system settings and manage which user accounts may do things like install software. This can also be applied to streaming services or games to control who is allowed to make purchases.

Secure Your Network

Ensure that your router and Wi-Fi network are protected by a strong password so your neighbors can't piggyback off of your connection. To take this a step further, consider creating a guest network for anyone who is not a member of your household. This will prevent others from potentially accessing anything personal.

Implement Parental Controls

For anyone with kids of any age, parental controls are a vital part of security and privacy. Modern devices and gaming consoles have some of these controls built in. There are also many services you can acquire that help parents keep kids safe by:

- ***Blocking or restricting access to specific websites or apps***
- ***Setting limits on device usage and screen time***
- ***Monitoring and managing online activity***

Prioritize Education

While access control policies are a great way to keep your household safe, education is equally important. Take time to discuss online safety with your household so everyone is aware of the dangers of sharing personal information and other potential threats to security and privacy.