SecurityAwarenessNews

the security awareness newsletter for security aware people

All About Access

Access Control and You

Access control defines how organizations manage systems, data, and entry points, both physical and digital. You can think of it as the rights granted to team members to perform tasks such as logging into a system or entering a secure area.

While management or system administrators are responsible for setting up access control policies, it's your responsibility to protect the access granted to you by those policies. Keep in mind that cybercriminals are always searching for ways to gain access to data, money, and people. Here's how you can avoid this:

Use Strong Passwords

A strong password is long, unique to each account, and meets organizational policies. Weak passwords can be easily cracked and allow an attacker to gain inside access to accounts and information.

Remember Physical Security

Access control is more than just a digital set of policies. Physical security is equally important, which includes:

- Locking workstations and devices when not in use
- Never allowing someone else to use your ID or badge to access secured areas
- Properly storing or securely disposing of any physical copies of private information
- Ensuring doors to secured areas remain closed and locked

Enable Multi-Factor Authentication (MFA)

MFA is a security feature that requires multiple authentication factors before granting access. The strength of MFA is that even if attackers steal a password, they're less likely to have access to the additional authentication methods. Therefore, the account or system in question will block their access.

Stay Alert for Phishing Attacks

Phishing is when a criminal sends an email or text to trick people into revealing passwords or opening dangerous links or attachments. A successful phishing attack can allow a criminal to take control of systems or accounts. Stay alert for common warning signs of these scams, such as threatening language, urgent requests, and unrealistic claims or promises.

The Importance of MFA

To do your job, your organization has given you special access to important systems, accounts, and data. Do you know who would also love to get that special access? Cybercriminals and scammers.

As always, one of the most important steps to stopping them is by using strong passwords.

Unfortunately, passwords aren't enough. They can be cracked or stolen through cyberattacks. This is why multi-factor authentication (MFA) is so important.

Why a Password Is Not Enough

Think of your password like a basic lock on your front door. It stops most people, but a skilled thief could still pick it. MFA is like adding a heavy deadbolt. Even if a thief picks the first lock, they are stopped in their tracks because they're less likely to be able to pick the heavy deadbolt.

Using MFA Securely

The additional authentication factors can be generated in a few different ways, including:

- A code sent via text message or email
- An alert on an authenticator app on your phone
- A physical USB key that you plug into your computer or tap on your device

Of those options, the USB key provides the best level of security, while email and text messaging provide the least security because they can be stolen. But they're all better than not using MFA.

Taking a few extra seconds to use MFA locks the access you have been granted. It protects your hard work, your team, and the organization. Be sure to follow your organization's policies for setting up required MFA, and consider turning it on for your personal accounts to protect your data.

Access Denied: The Threat of Ransomware

While preventing attackers from accessing systems and data is important, there is another side to the story: Ensuring authorized users can always access the tools and data they need.

Think about it like this. Imagine you work at a doctor's office and need patient records to provide care. One day, you come into work and are suddenly unable to open those records because a criminal hacker has locked you out. Even worse, every computer in the office has been completely blocked.

How would you do your job? In many of these cases, you couldn't, and neither could any of your co-workers.

This scenario highlights a major threat that is one of the most common and dangerous in modern workplaces: ransomware. Here's what you need to know about it.

What Is Ransomware?

It's a type of malicious software (malware) that is designed to lock data and knock systems or services offline. The attackers then demand an expensive payment (the ransom) from the organization to restore access. To add pressure, the attackers often steal the data first, then threaten to leak it.

How Do Ransomware Infections Happen?

There are many ways a computer or system can get infected, but one of the most common is through phishing attacks. Phishing uses emails or messages to trick people into opening harmful links or attachments, opening the door for attackers.

What Can You Do To Help Prevent Ransomware Infections?

Since most infections are spread by phishing attacks, stay alert for warning signs, such as threatening or urgent requests, in all forms of communication. Never open unexpected links and attachments. Follow your organization's security policies, and if you notice anything suspicious, report it immediately!

Remember, access is everything. We need to protect it against unauthorized people. And maintain it for authorized people.