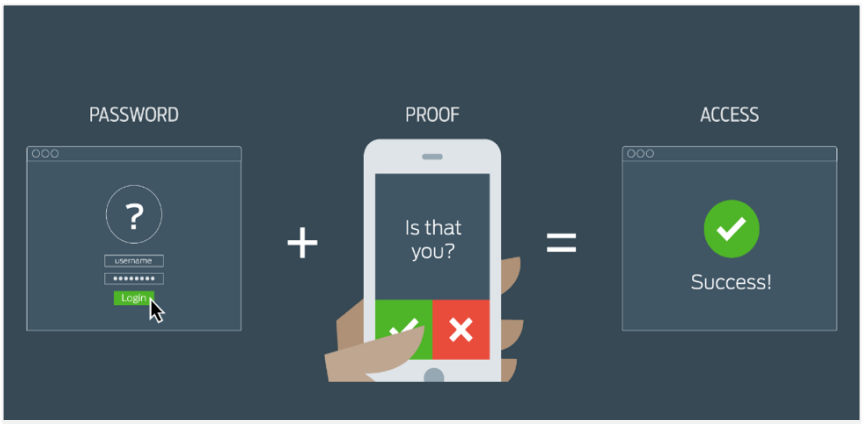
Why Must I Log-In Twice?

The Importance of Multi-Factor Authentication

The cybersecurity outlook for education is a little scary. Microsoft Security Intelligence spotlights education as the industry at highest risk for malware encounters based on their worldwide tracking metrics. Nearly two-thirds of malware encounters identified by Microsoft were from the education sector alone. That figure represents more than 5.7 million devices at risk over a 30-day period. (Microsoft, 2021)



This data begs the question, "Why schools?" What is it about education that makes the industry so vulnerable to cyber-attack? The attraction is likely twofold. First, the kinds of data schools need to collect for normal operations have a resale value. Scores of personally identifying information, including home addresses, names and birthdays all linked to real people are a windfall in the wrong hands. Most schools store this data and more. Second, the nebulous nature of cyber threats vs. more concrete physical safety and security concerns understandably pulls focus and funding away from cybersecurity. It is easy to put off cybersecurity improvements because the threat seems distant, but the resulting technological lag creates an opportunity that cyber attackers can, and do, exploit.

The good news is that keeping cyber attackers out of your systems starts with the simple act of "locking" your cyber front-door. Requiring a username and password, or single-factor authentication, is the cyber equivalent of leaving a closed door unlocked. It may keep out minor threats but does very little against anything more advanced. Just as you would secure your home with a deadbolt, requiring multiple authentication measures to gain access to your system helps ensure only verified users can get in.

Weaknesses of Single-Factor Authentication

Single-factor authentication, requiring users to provide just one "proof" that they are the intended user, is currently the most common form of cyber identity verification. Single-factor authentication is easy to implement, however, it is also easy to deceive. Cyber attackers often need only identify a matching username and password pair for access, and the methods for doing so are surprisingly numerous. Recycled usernames and passwords from previous data breaches, phishing schemes, key loggers, and other malware all have the potential to overcome single-factor authentication systems with relative ease, open that "door", and gain entry.

The United States Cybersecurity and Infrastructure Security Agency (CISA) identifies single-factor authentication practices as one of three "bad practices" that could open an organization to cyberattack and says that fixing authentication issues alone "can dramatically improve resilience against common cybersecurity threats" (CISA,2020).

How is Multi-Factor Authentication Different?

Unlike single-factor authentication, multi-factor authentication requires at least two distinct authentication measures to verify a user's identity. Think of this as closing a door and locking the deadbolt. For example, a program that requires you to enter a password and verify a chain of numbers texted to your cell phone is using a weak form of multi-factor authentication. In this case, a would-be hacker would need to identify a matching password/username combination and access or hijack the specific phone number associated with that account to gain entry.

Why Must I Log-In Twice?

Multi-factor authentication in general is significantly more secure than single-factor authentication since cyber attackers must get information from two or more separate sources for access. Because of this, all multi-factor authentication methods are considered relatively strong. However, some measures are better than others. Cell phone numbers, for instance, are not immune from hacks themselves, meaning a cyber attacker could presumably pull together both factors and gain access to the system in the example above.

According to CISA, authentication methods that require users to be in possession of a specific object, such as a smart card, security token, a key fob, or a method that requires users to prove a unique physical trait, such as a fingerprint, provide the highest level of security (CISA,2020). Apps installed on cell phones can replicate the added security of many of those methods without requiring an additional piece of hardware, since most people already have compatible cell phones.

Where Should I Start?

Making changes to your IT operations can certainly be a daunting task, no matter your organization's size, however securing your systems is the only way to keep your sensitive data safe. CISA provides a comprehensive Capacity Enhancement Guide on implementing strong authentication that walks through steps and considerations one-by-one. It is available online at cisa.gov and cited below.

While requiring multi-factor authentication is an important step in any cybersecurity plan, it is important not to overstate its value. Even the best multi-factor authentication systems only represent one part of an effective cybersecurity strategy and schools should ensure they have a comprehensive plan in place to keep staff and students' information safe. We recommend Members to reach out to CSDSIP for guidance and specific coverage information related to cyber vulnerabilities.

References

CISA. (2020, October 8). *Capacity Enhancement Guide on Implementing Strong Authentication.* Retrieved from Cybersecurity and Infrastructure Security Agency : https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508_1.pdf

Microsoft. (2021, September 1). *Most Affected Industries* . Retrieved from Microsoft Security Intelligence: https://www.microsoft.com/en-us/wdsi/threats

303.722.2600
www.csdsip.org
: @CSDSIP