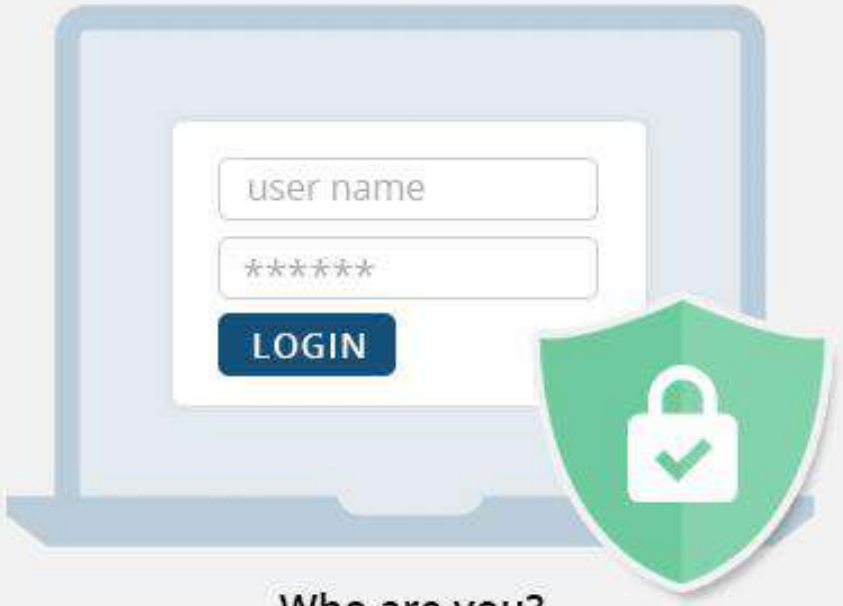
AUTHENTICATION AND AUTHORIZATION

Authentication



Who are you?

Validate a system is accessing by the right person

Authorization

Are you allowed to do that?

Check users' permissions to access data

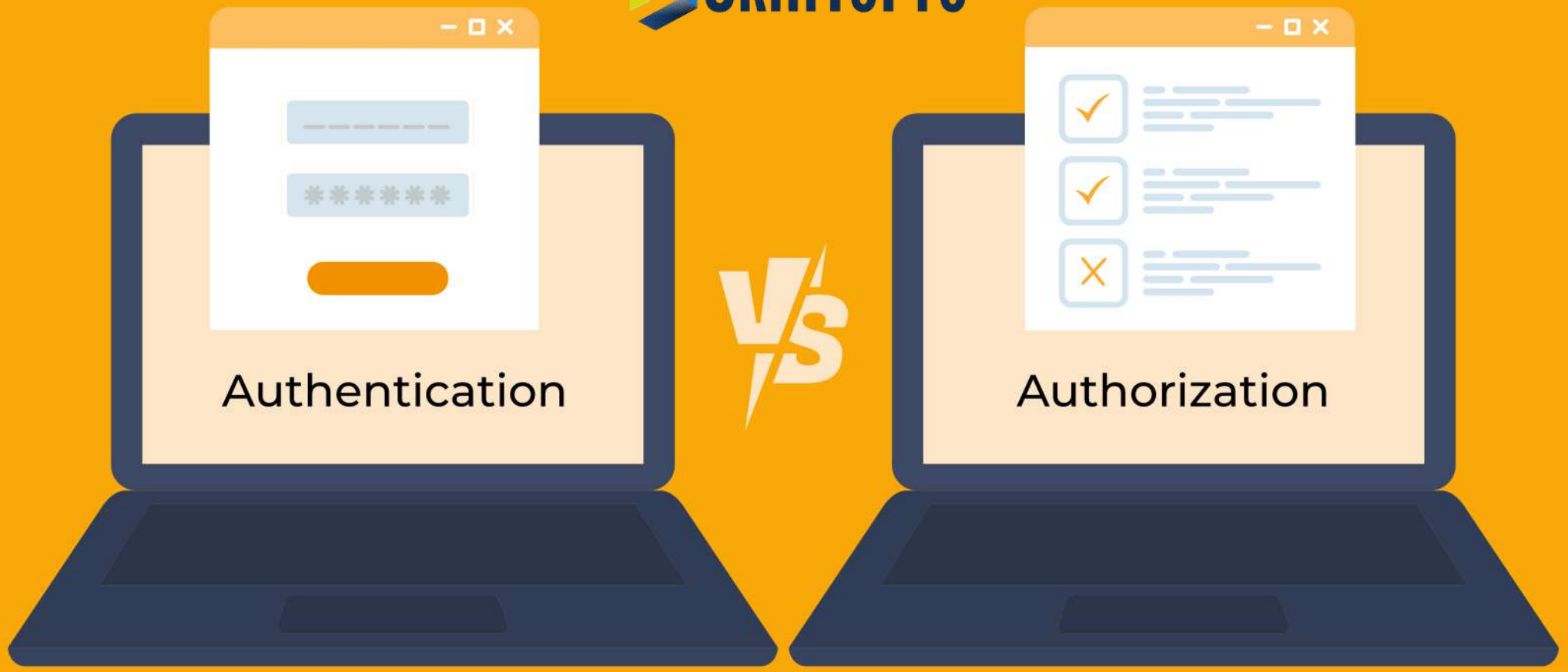
AUTHENTICATION AND AUTHORIZATION

As a Cybersecurity professional, one of the most important things you do is to ensure that only authorized individuals gain access to information, systems, and networks under your protection. You use access controls to provide this assurance.

ACCESS CONTROL PROCESS

- **Identification** - in identification, an individual makes a claim about their identity.
- **Authentication** - proof comes into play during the second step of the process: authentication.
- **Authorization** - Just proving your identity isn't enough to gain access to a system. The access control system also needs to be satisfied that you are allowed to access the system.
- **Accounting** - access control systems also provide an accounting functionality that allows administrators to track user activity and reconstruct it from logs.

SkillToPro



PHYSICAL ACCESS CONTROL PROCESS

SkillToPro

DIGITAL ACCESS CONTROL

Digital Access Control (DAC) is a security system that uses electronic measures to restrict access to physical locations, data, or IT systems. It is a more advanced and versatile alternative to traditional mechanical locks and keys, offering a number of advantages such as:

- **Enhanced Security**: DAC systems use electronic credentials such as key cards, fobs, or biometric identifiers (fingerprints, iris scans) to verify user identity before granting access. This makes it much more difficult for unauthorized individuals to gain access, compared to traditional methods that can be easily picked or copied.

DIGITAL ACCESS CONTROL

- **Increased convenience:** DAC systems are more convenient to use than traditional locks and keys. Users don't need to worry about losing keys or carrying around multiple keys for different doors. They can simply present their credential to the reader and gain access.
- **Improved auditability:** DAC systems can track and record who accessed what, when, and where. This information can be used to investigate security incidents or identify potential security risks.
- **Greater flexibility:** DAC systems can be easily programmed to grant or deny access based on a variety of factors, such as time of day, day of the week, or user group. This allows for more granular control over access than is possible with traditional methods.

DIGITAL ACCESS CONTROL - TYPES

There are a number of different types of DAC systems available, each with its own advantages and disadvantages. The most common types include:

- **Card access control systems:** These systems use key cards or fobs to identify users.
- **Biometric access control systems:** These systems use biometric identifiers such as fingerprints, iris scans, or facial recognition to identify users.
- **Mobile access control systems:** These systems use smartphones or other mobile devices to identify users.

The best type of DAC system for a particular application will depend on a number of factors, such as the level of security required, the budget, and the convenience needs of the users.

PASSWORD POLICIES & REQUIREMENTS

SkillToPro

When you set a password policy for your organization, you have a number of technical controls available that allow you to set requirements for how users choose and maintain their passwords. This section discusses a few of those mechanisms.

- **Password Length -** This is simply the minimum number of characters that must be included in a password. It's good practice to require that passwords be at least eight characters, or even longer passwords. The longer a password is, the harder it is to guess.
- **Password Complexity** – These are requirements enforced on users to include different types of characters in their passwords, such as uppercase and lowercase letters, digits, and special characters. Just as with password length, the more character types there are in a password, the harder it is to guess.

PASSWORD POLICIES & REQUIREMENTS

SkillToPro

- **Password Expiration** - Password expiration requirements force users to change their passwords periodically. For example, an organization might set a password expiration period of 180 days, forcing users to change their passwords every 6 months.
- **Password History** - Password history requirements are designed to prevent users from reusing old passwords. Most authentication systems are configured to remember the previous passwords used by each user and prevent them from reusing that password in the future.
- **Password Resets** - Every organization should allow users to change their passwords quickly and easily. One point of caution is that organizations should carefully evaluate their password reset process for users who forget their passwords. If they're not designed well, these processes can provide an opportunity for attackers to gain access to a system by performing an unauthorized password reset.

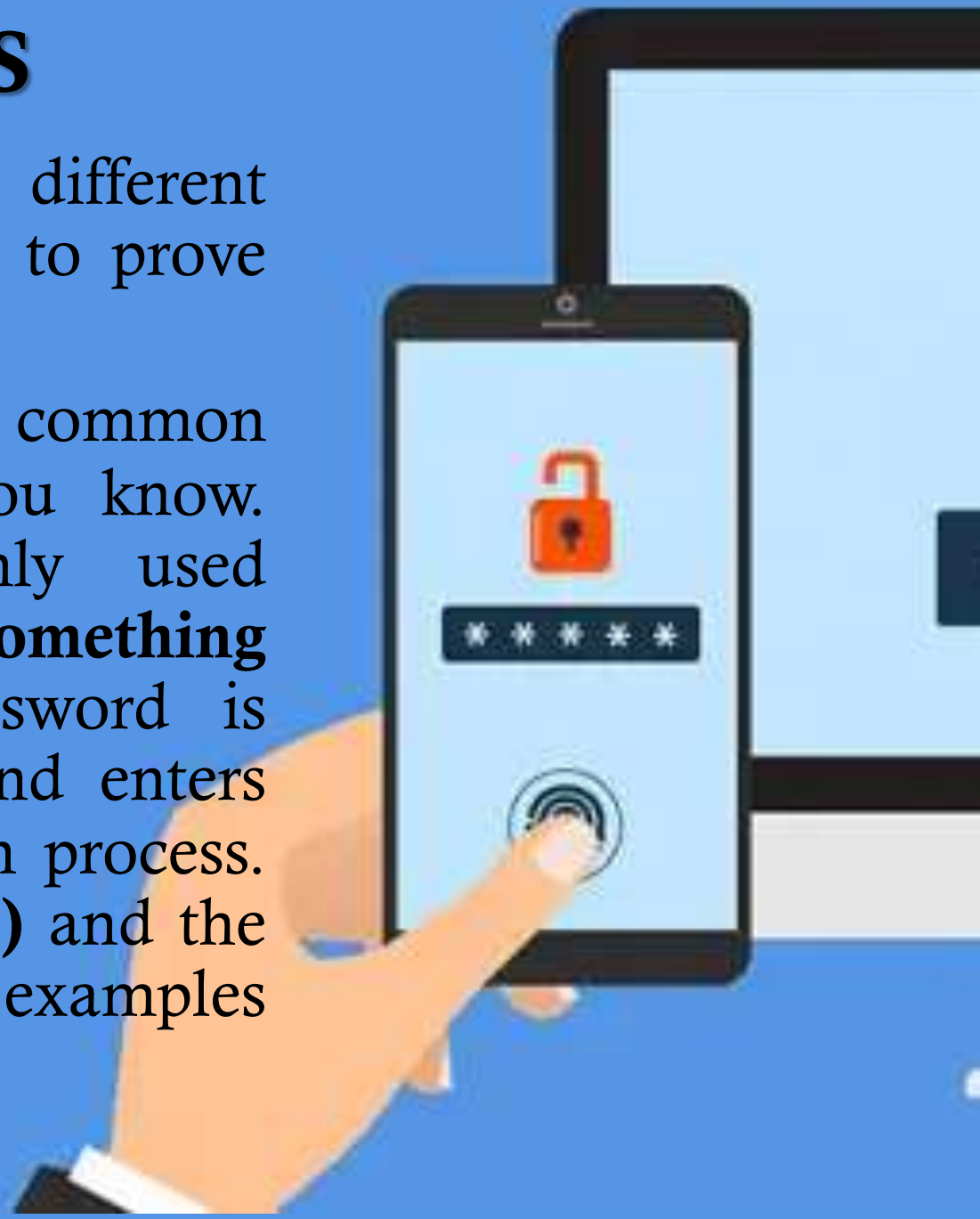
Password Policies & Requirements

- **Password Reuse** - IT teams should also strongly encourage users not to reuse the same password across multiple sites. This is difficult to actually enforce, but it does provide a strong measure of security. If a user reuses the same password on many different sites and one of those sites is compromised, an attacker might test that password on other sites, hoping that the password owner reuses the same password.
- **Password Managers** - It's difficult for users to manage unique passwords for every site they visit. That's where password managers play a crucial role. These valuable tools are secure password vaults, often protected by biometric security mechanisms that create and store unique passwords. They then automatically fill those passwords on websites when the user visits them. That way users can have unique, strong passwords for every site they visit without having to remember them all.

AUTHENTICATION FACTORS

Computer systems offer many different authentication techniques that allow users to prove their identity.

- **Something You Know-** the most common authentication factor is something you know. Passwords are the most commonly used authentication technique. This is a **"something you know"** factor because the password is something that the user remembers and enters into a system during the authentication process. **Personal identification numbers (PINs)** and the **answers to security questions** are also examples of something you know.



AUTHENTICATION FACTORS

- **Something You Are** - The is the behavioral attribute of the user. Biometric authentication techniques measure one of your physical characteristics, such as a fingerprint, eye pattern, face, or voice.
- **Something You Have** – It requires the user to have physical possession of a device, such as a smartphone running a software token application or a hardware authentication token key fob. These devices generate onetime passwords that are displayed to the user and allow them to prove that they have access to a physical device. Similarly, smart cards can serve as a "something you have" factor, requiring that the user insert a card with a digital chip into a specialized reader.

MULTI-FACTOR AUTHENTICATION

A good solution to authentication compromise is to combine authentication techniques from multiple factors, such as **combining something you know with something you have.** This approach is known as multi-factor authentication (MFA). Example is passwords and smart cards. When implementing multi-factor authentication, it's important to remember that the techniques must be different factors.