What is passwordless authentication?

Many employees, whether in the office or working from home, use a variety of applications to perform their everyday tasks. A lot of these applications require passwords before an employee can access them. Because of this, users are compelled to memorize and manage multiple passwords to keep sensitive information safe.

Unfortunately, many users find that keeping track and constantly changing their passwords is both overwhelming and tedious. This leads many employees to adopt risky password habits such as using weak passwords, using the same passwords for multiple accounts and applications, and writing down passwords on sticky notes where everyone can see them.

Cybercriminals can take advantage of this risky behavior to launch cyberattacks on unsuspecting organizations and steal their confidential information. In fact, Verizon's 2021 Data Breach Investigations Report reveals that compromised login credentials are one of the leading causes of data breaches.

There are various ways hackers can steal login credentials:

- **Phishing** - an attack that uses fake email or SMS messages to convince users to go to a compromised site, download malware, or provide their private information.
- **Credential stuffing** - hackers use stolen credentials to gain access to user accounts or network resources. Credential stuffing takes advantage of the fact that many people use the same passwords for different accounts.
- **Brute force attacks** - a method where attackers bombard a system with various login combinations to find the correct credentials that will give them access to that system's information and resources.
- **Man-in-the-middle attacks** - an attack where hackers try to intercept the communications between two parties to either eavesdrop, corrupt data, sabotage communications, or steal private information.
- **Keylogging** - uses a program called a keylogger to monitor and capture a user's keystroke on the keyboard.

One way of reducing the risk of having your credentials stolen and experiencing a data breach is by using passwordless authentication.

Passwordless authentication

Passwordless authentication is a process of verifying a user's identity without the need for a password. Instead, a user can provide alternative forms of authentication, such as:

- **Biometrics** - Uses the unique physical traits of a user, such as a fingerprint, retinal scan, or facial recognition to verify their identity.
- **One-time passcodes (OTP)** - A method that requires users to enter a code every time they log in. This code is usually sent through text message or email.
- **Push notifications** - Employees logging into their accounts will receive a push notification from an authenticator app on their mobile device. All they need to do is open the authenticator app via a push notification to verify their identity.

Passwordless authentication is commonly used in conjunction with Single Sign-On applications and multifactor authentication to ensure the highest level of security.

Advantages of passwordless authentication

Using passwordless authentication provides a host of benefits:

1. Eliminates the risk of password theft

Phishing is one of the most common cyberattacks designed to steal valuable information, including login credentials. In fact, 36% of data breaches reported in 2021 were the direct result of phishing attacks.

Passwordless authentication uses advanced authentication technology which eliminates the need for passwords. This protects your employees from being exploited by cybercriminals through phishing attacks.

2. Enhances supply chain security

Using passwordless authentication prevents unauthorized individuals from accessing and installing malware into your company network. This method is ideal for preventing software supply chain attacks, which can greatly enhance your organization's supply chain security.

3. Improves employee productivity

Generating, monitoring, storing, and updating multiple passwords can take up a lot of an employee's time. Additionally, employees can spend valuable time requesting IT helpdesk to reset their passwords. This can make employees feel frustrated, which can affect their productivity.

Passwordless authentication offers a more convenient and secure authentication option that allows users to quickly gain access to the resources they need. This eliminates the frustration of managing passwords and improves overall productivity.

Using passwordless authentication is a good way to improve your organization's cybersecurity defenses. Another way is to partner with a trusted managed IT services provider like Safebit Solutions Inc. Our cybersecurity solutions will keep your data safe from malicious cybercriminals. Call us now to learn more.