Cyber Liability

The Importance of Two-factor Authentication

As cyber attacks become more and more common, protecting your data is increasingly difficult. In fact, a study from Juniper Research found that by 2023, cyber criminals are expected to steal an estimated 33 billion records. In light of the growing number of cyber attacks, many companies are turning to two-factor authentication (also commonly called 2FA or multifactor authentication) to enhance their cyber security.

While no cyber security method is foolproof, using two-factor authentication can add an extra layer of security to your online accounts. So how exactly does two-factor authentication work?

What Is Two-factor Authentication?

While complex passwords can help deter cyber criminals, they can still be cracked. To further prevent cyber criminals from gaining access to employee accounts, two-factor authentication is key. Two-factor authentication adds a layer of security that allows companies to protect against compromised credentials. Through this method, users must confirm their identity by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate applications, networks and servers.

With two-factor authentication, it's not enough to just have your username and password. In order to log in to an online account, you'll need another "factor" to verify your identity. This additional login hurdle means that would-be cyber criminals won't easily unlock an account, even if they have the password in hand. A more secure way to complete two-factor authentication is to use a time-based one-time password (TOTP). A TOTP is a temporary passcode that is generated by an algorithm (meaning it'll expire if you don't use it after a certain period of time). With this method, users download an authenticator app, such as those available through Google or Microsoft, onto a trusted device. Those apps will then generate a TOTP, which users will manually enter to complete login.

Why Two-factor Authentication and Password Management Is Important

As two-factor authentication becomes more popular, some states are considering requiring it for certain industries. It's possible that as cyber security concerns continue to grow and cyber attacks become more common, other states will follow suit. Even if it's not legally required, ongoing password management can help prevent unauthorized attackers from compromising your organization's password-protected information. Effective password management protects the integrity, availability and confidentiality of an organization's passwords.

Above all, you'll want to create a password policy that specifies all of the organization's requirements related to password management. This policy should require employees to change their password on a regular basis, avoid using the same password for multiple accounts and use special characters in their password.