Multi-factor Authentication for Law Firms 101

A username and password are enough for many sites, this single-factor authentication is often used for retailers and other such sites. However, more sensitive data, like the information law firms store, should be guarded by multi-factor authentication. Hackers can access a lot of information with just a username and password, including a social security number, bank or credit card information, medical records, and more. On top of that, many people use a similar username and password across sites, so if a hacker gets one, they may get them all.

This scenario is one that law firms simply can’t risk. As cyberattacks continue to rise, it’s imperative for law firms to educate themselves and utilize the cybersecurity resources available to protect their business.

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) requires one factor, such as a password, that’s combined with another factor, such as a code, a device, or other personal identifiers like biometrics or voice recognition. Even with these parameters, a long, intricate password that is difficult to trace is still important. Generally, a good password consists of 20+ characters or a phrase that can be very strong, yet easy for the user to remember. Hackers want quick "attacks," so the goal is to create a long enough password that creates more work and is difficult to guess.

It's important to remember that no password is fail-safe, which is why MFA is important. It is an extra layer of protection that is difficult for a cyberattacker to have access to.

Why Law Firms Should Enable Multi-Factor Authentication

Some firms think security is reserved for large and prominent law firms, but it's actually more common for small firms to experience a breach. For one, there are more small or solo firms, and they often don't have the resources or team to handle their security.

A firm with Office 365 or Google Suite can enable 2FA quickly and easily. Employees will not need to go through the two-factor process for each log-in. Instead, 2FA is required for each login attempt from a new device. 2FA requires additional verification every so often, but it's far more convenient than dealing with a breach and the possible business, legal, and reputational harm.

Incorporate Legal Technology in Your Firm's Cybersecurity Strategy

Utilizing law practice management software is a simple way to secure your law firm's data. Using cloud-based software, like Bill4Time, performs automatic routine updates to ensure the platform is always up to date. Out-of-date software is a common source for cyberattacks because it creates a weak point for hackers to enter.

Bill$Time also offers customized security measures like MFA. This change can only be done by users with access to firm-wide settings, such as a firm administrator. Similarly, administrators can configure the user permission settings and access for every function. Permissions and access for each task and each user can be customized, including temporary access for contractors. Administrators can also track logins automatically, so if there is a breach, it's easier to pinpoint.

Multi-Factor Authentication and Your Firm’s Email

An email account is among the most important accounts for law firms – and anyone else – to protect. More times than not, an email provides avenues to access other accounts. Password recovery is often tied to emailing a link to reset a password. If an email account is compromised, all the account passwords could be reset.

With two-factor authentication (2FA) enabled on an email, a hacker would need access to both the email account and a smartphone or other device. This added step reduces the risk of hackers not only gaining access to email but potentially resetting other passwords.

If a device like a smartphone or a tablet is used for authentication, it’s important that they’re also protected with a PIN or fingerprint. Again, this is about creating layers of security. Like email, having access to a phone, whether it’s stolen or hacked, gives someone access to an array of accounts and information.

Outlook on Multi-factor Authentication for Law Firms

Data breaches happen, but with preparation, they can be prevented or controlled. Law firms can protect their sensitive information by creating obstacles for cyber attackers like difficult, frequently changed passwords, user access controls, and multi-factor authentication.