



Common Two-Factor Authentication (2FA) Solutions

By William Pate

At Innovative Computing Systems, we promote a cybersecurity perspective called “*defense-in-depth*.” Essentially, we believe law firms, legal departments and individuals need more than one or two layers of information security. Users and clients must be confident that even if one defense fails, another will stand up and attempt to prevent or mitigate an attack. We have long recommended that clients utilize two-factor authentication as one of those layers of defense.

Two-Factor Authentication (2FA)

Two-factor authentication is the use of two different means to verify your identity.

With 2FA, a user who attempts to log on to a workstation or to access protected programs and/or files is prompted to identify him- or herself via a second factor. This is done by a means other than that same computer and login/password combination, such as using one’s smartphone with an SMS text message, a hard token or even a phone call. Two-factor authentication is simply another way to make sure that the user is the expected individual by requiring another form of identification. It’s the technological version of two checkpoints instead of one.

For users not concerned with the under-the-hood aspects of the security being provided, the factors used to authenticate a session are the most important components of 2FA. Given the variety, it is important to be discerning in choosing your law firm’s two-factor authentication solution. You must ensure your chosen

solution will integrate with all your firm’s applications, provide the expected security and be user-friendly. Let’s examine a few of the options.

Email and SMS Message

One of the most common forms of two-factor authentication is the email or SMS message. Many people have lost their passwords and requested to have them reset—only to be told to enter a code received via text message or email. This is an example of two-factor authentication.

PROS: Almost everyone has an email address and/or SMS-enabled phone.

CONS: You may not use SMS or you do not have access to your email.

Applications

Some firms use mobile device applications as a second layer of password security. For instance, many of Google’s services require users to download the Google Authenticator app, generate a code and enter it at the workstation within a defined period to access certain information.

Similarly, we consider our partners at Duo to offer a best-in-breed enterprise-quality 2FA solution. Duo allows one to simply press an “Approve” button on his or her device to verify identity.

Other solutions require users to enter their username and password at the workstation and then input a number generated by an app on their phones or tablets. Users have a limited time to enter the number before it expires and a new one must be generated and entered.

PROS: People always have their smartphones with them.

CONS: In the event the user should lose his or her phone, access could prove difficult. Transferring the number from the smartphone to the computer can be a hassle and prevent one from logging in if time runs out.

Security Tokens

Security tokens are physical devices made solely for the purpose of providing 2FA. Some tokens display a number to input as a passcode when logging on at a workstation. Other tokens will connect to the workstation via Bluetooth. Dongles, which you insert into an access point, are also popular forms of 2FA.

PROS: The devices are often rugged and always ready to provide access.

CONS: If the devices are lost or forgotten or the power source dies, the ability to authenticate and gain access may be hampered.

Considerations

Two-factor authentication is no longer an expensive cybersecurity solution. With cloud-based 2FA platforms, implementation and onboarding can be accomplished rapidly and easily. Best of all, the low cost now puts powerful 2FA solutions within reach of all law firms.

If you would like to learn more about improving your firm's cybersecurity with enterprise-quality 2FA solutions, contact us at sales@innovativecomp.com.

About Innovative Computing Systems, Inc.

Since 1989, Innovative Computing Systems has primarily focused on the technology needs of law firms and legal departments. Innovative Computing Systems skills are also sought out by entities such as municipalities, corporate environments and professional services industries. Innovative Computing Systems takes a best-of-breed approach to all its offerings by selecting only premier technology partners to provide solutions for our clients. We are committed to maintaining long-term strategic relationships with clients to ensure the highest levels of success with IT initiatives. Learn more by visiting www.innovativecomp.com.