MULTIFACTOR AUTHENTICATION

Increase Login Security with Flexible Multi-factor Authentication Solutions.



Sandbox Technologies
3868 W Carson St, Suite 316
Torrance, CA 90503
www.sandboxtech.com
Tel. 424.207.5130

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Multifactor Authentication

Help prevent network break-ins by making user authentication more secure.

In a business environment where user login credentials are commonly cracked, sold, and used for nefarious reasons, simple username-password combinations are no longer enough. Multifactor authentication is an essential protection that ratchets that no business should be without.

Passwords Alone Aren't Secure

Identity security is one of the most significant challenges IT organizations face. The primary tool most companies use to permit network access is the username-password combination. Unfortunately, passwords are a weak link in the security chain. First, relying on users to create individual, complex passwords to all their accounts is an uphill battle. More often than not, the same password is used across multiple sites, creating a possible domino effect where multiple accounts become vulnerable as a result of just a single password being cracked. Second, no matter how complex or unique passwords are, they can still be compromised through data breaches, malware, and device theft.

Multifactor authentication steps up security by requiring users to present a combination of two pieces of "evidence" when logging into an account: something they know, such as a password; something they have, such as a mobile device; or something they are, such as a fingerprint. In this way, multifactor authentication helps protect against phishing, social engineering and brute-force password attacks.

Flexible Solutions

Sandbox Technologies' offers a variety of multifactor authentication solutions, which vary according to platform and software requirements. Our most popular tool pushes notifications to users for approval to verify their identity. Other options include using Universal 2nd Factor (U2F) security tokens, USB hardware tokens, mobile passcodes, as well as less secure solutions (when no alternative exists) such as SMS, phone callback, and biometrics.

The primary tool most companies use to permit network access is the username–password combination. Unfortunately, passwords are a weak link in the security chain.

Multifactor authentication can help to secure both on-premises and cloud applications, and should be considered one of today's single most important security implementations that no organization should be without.

For more information, or to discuss your security needs, contact your Sandbox Technologies Engineer or Consulting CIO, or send an email to projects@sandboxtech.com.