UNIVERSAL DATA INCORPORATED

Multifactor Authentication

Keep your employee login credentials out of the hands of cybercriminals

Imagine how much damage could be done if a cybercriminal gained access to one of your employee's passwords. Now, consider the unfettered access that the same criminal would have if they could figure out or steal admin-level login credentials.

There was a time when a username and password were enough for most business applications, but no more. Today's bad actors utilize every trick in the book to steal login information and use it against companies like yours.

Our team uses multifactor authentication to protect your business, even if a careless employee inadvertently allows criminal eyes to discover their access credentials to company systems.

What is multifactor authentication?

Multifactor authentication, sometimes called "MFA" or "2-Factor Authentication," is a tool that we use to double-check the person's identity trying to log into your systems, applications, online assets, and cloud-based infrastructure. Multifactor authentication is the second line of defense for access into your systems, checking for an alignment of three identifiers or "factors."

- Knowledge — something only the user would know (PINs, answers to questions)
- Possession — something the user has (like email or smartphone)
- Inheritance — something the user is (biometric data)

The business benefits of implementing multifactor authentication

- Assists in keeping careless employees from becoming a risk to your organization
- Builds out a secondary layer of systems access protection
- Guards against data theft
- Helps to conform to compliance standards

Think you can protect your usernames and passwords?

We have every confidence in the care you and your employees put into guarding your login credentials.

What concerns us—and should worry you—is the massive breaches of login credentials happening to vendors.

For example, a breach of a customer support database of one of the world's leading software companies recently exposed 280 million customer records.1

Breaches like this are far too common and give the bad actors easy access to the credentials you use on vendor portals, potentially opening doors to your IT assets.

An extra step that makes a big difference

Multifactor authentication is now required by banks and eCommerce portals and legislative/industry-standards compliance. As cybercriminals become more sophisticated, even small businesses must be on guard. The extra second or two it takes to use multifactor authentication to access your company systems is far better than dealing with stolen data, systems damage, or extended downtime caused by criminals leveraging stolen login credentials.

Need more information?

Universal Data, Inc.

https://www.udi.com/

info@udi.com

504-934-7120

References:

[1](Source: https://www.varonis.com/blog/data-breach-statistics - accessed 2022/02/01)