THE MILLER GROUP
TECHNOLOGY SOLUTIONS

Solutions & Success
The Inside Story

How The Miller Group Enhanced This Firm's Password Security

www.themillergroup.com

Maintaining strong and complex passwords may sound easy in theory, but in reality, most users opt for easy-to-remember passwords instead.

Multi-factor authentication *(MFA)* is a great way to overcome the users' resistance to maintaining strong passwords, while still ensuring adequate standards of cybersecurity.

That's why this marketing firm hired The Miller Group. They needed a reliable layer of security for their users' logins, and MFA was the perfect solution.

The Unfortunate Reality Of Password Security

Despite the fact that passwords are the most direct way to access a user's private information, most passwords in use today are simply not strong or complex enough.

Passwords protect email accounts, banking information, private documents, administrator rights and more—and yet, user after user and business after business continue to make critical errors when it comes to choosing and protecting their passwords.

To be fair to users, there's a lot to keep in mind when choosing a password:

Length and Complexity

Keep in mind that the easier it is for you to remember a password, the easier it'll be for a hacker to figure it out. That's why short and simple passwords are so common - users worry about forgetting them, so they make them too easy to remember, which presents an easy target for hackers.

Numbers, Case, and Symbols

Another factor in the password's complexity is whether or not it incorporates numbers, cases, and symbols. While it may be easier to remember a password that's all lower-case letters, it's important to mix in numbers, capitals, and symbols in order to increase the complexity.

Personal Information

Many users assume that information specific to them will be more secure - the thinking, for example, is that your birthday is one of 365 possible options in a calendar year, not to mention your birth year itself. The same methodology applies to your pet's name, your mother's maiden name, etc.

However, given the ubiquity of social media, it's not difficult for hackers to research a target through Facebook, LinkedIn, and other sites to determine when they were born, information about their family, personal interests, etc.

Pattern and Sequences

Like the other common mistakes, many people use patterns as passwords in order to better remember them, but again, that makes the password really easy to guess. **"abc123"**, or the first row of letters on the keyboard, **"qwerty"**, etc., are extremely easy for hackers to guess.

In the end, creating and using strong passwords can be frustrating—the more secure they are, the more difficult they are to remember. The more memorable they are, the greater threat they pose to the business.

How Did The Miller Group Help This Marketing Firm?

The Miller Group carefully planned and executed a project to enable MFA for this marketing firm's environment. By implementing a robust MFA solution, we would enhance the security of their passwords and authentication.

The specific services in use by this client they are protected with MFA include:

- Local computer logins
- Connections to Office 365
- VPN connections

We used industry-leading MFA solution Duo, which requires each user to add a device for secondary authentication *(covering one or more of the following: modern smartphones for push approvals, time-based codes by text, time-based codes by phone call, or token devices).*

Furthermore, their conference room computer was isolated on a guest network that also included this marketing firm's wireless network.

Enforcing the use of Duo MFA by requiring approval of the login through a cell phone or physical hardware key resulted in increased confidence that this marketing firm will stay safe from cybercriminals.

MFA: The Better Way To Approach Password Management

MFA is a superior way to keep your data more secure—after all, it blocks 99.9% of identity-based attacks.

MFA requires the user to utilize two methods to confirm that they are the rightful account owner. There are three categories of information that can be used in this process:

- **Something you have:** Includes a mobile phone, app, or generated code
- **Something you know:** A family member's name, city of birth, pin, or phrase
- **Something you are:** Includes fingerprints and facial recognition

The Benefits Of MFA

Bring Your Own Device

In today's modern business world, more and more employees prefer to do at least some of their work through their mobile devices, which can present a serious security risk. However, with an MFA solution, you can enroll new employee devices in minutes, given that there's no need to install an endpoint agent.

Convenient Flexibility

A MFA solution won't force you to apply the same security policies to every user in the company. Instead, you are given the capability to specify policies person by person or group by group.

How Does A Multi-Factor Authentication Solution Work?

1. User logs into the session with primary credentials.
2. The session host validates credentials with Active Directory.
3. Then, it sends credential validation to the cloud via the login app.
4. The MFA client sends its secondary authentication to the user. User approves.
5. The MFA client sends approval back to the session host via the login app.
6. The user accesses their session very securely.

Though MFA does make it harder for the account owner to access the account, it also makes it difficult for cyber thieves to learn your password. Their job becomes much tougher because they now need to do more than just hack your password. They'll need personal information about the account owner.

With so many accounts being too easy to break into, hackers are more likely to just move on instead of trying to break through the multiple-factor authentication process.

The Miller Group Will Help Protect Your Data

If you're unsure about how to implement an MFA solution, don't try to handle it all on your own.

The Miller Group will help you evaluate your password practices and security measures as a whole to make sure you're not taking on any unnecessary risks. We will guide you in implementing MFA for your entire staff, ensuring your data is properly protected, just like we did for this marketing firm.

Contact our team and arrange a consultation.