TECHNIJIAN
technology as a solution

SOLUTIONS & SUCCESS

The Inside Story

2022

Don't Assume Your Microsoft 365 Data Is Secure

A client of ours was at risk of being permanently banned by Microsoft because they didn't have the right cybersecurity measures in place. Do you know how to maintain security in Microsoft 365?

Should You Be Worried About Microsoft Office 365 Security Capabilities?

Yes and no.

As a rule, you should always be concerned about security. Cybersecurity is a never-ending battle, and as such, it should always be considered when it comes to the technology you use at your nonprofit. But what about Microsoft Office 365?

Designed according to Microsoft Security Development Lifecycle, Microsoft Office 365 is a Software-as-a-Service solution that uses a defense-in-depth approach to provide physical, logical, and data layers of security features and operational best practices. Plus, it offers enterprise-grade user and admin controls to further secure your environment.

You Play A Key Role In Cybersecurity

Regardless of how many security capabilities Microsoft 365 offers, they won't amount to anything if you don't use them.

That was the issue with this client. In order to keep things simple, they had failed to follow cybersecurity best practices. Users had repeated and simple passwords and weren't protecting their accounts with multi-factor authentication *(MFA)*.

Eventually, this led to a security breach. In response, Microsoft locked this client's business out of their email system for four days and threatened to permanently ban them from Microsoft 365 unless they took action to address their vulnerabilities.

How We Helped This Client Secure Their Microsoft 365 Accounts

Our team's first step was to implement MFA on all Microsoft 365 accounts. This is another way that Microsoft 365 keeps your data secure.

MFA requires the consumer to utilize two methods to confirm that they are the rightful account owner. By setting up these types of verification, you add an extra layer of security to your business' Microsoft Office 365 accounts.

Users must acknowledge a phone call, text message, or app notification on their mobile device after correctly entering their work account password. They sign in with their password *(step 1)*, and a code sent to their phone *(step 2)*. That extra layer of protection will mitigate the vast majority of unauthorized login attempts.

In order to still keep things simple for the client, we took the extra step of whitelisting logins on their office network. This ensured that MFA would only trigger on login attempts from outside the office.

Furthermore, we began managing a range of key cybersecurity maintenance tasks for the client:

- Reviewing logs to monitor for breach attempts.
- Maintaining MFA
- Monitoring Microsoft Exchange connectors for suspicious activity

Enlist An Expert Team To Manage Your Microsoft 365 Security

Make sure your organization is fully leveraging your investment in Microsoft 365 and deploying the security features you already own or are not aware of, to help improve your security posture.

As your experienced partner, Technijian will help you identify risk and enhance security within your Microsoft 365 environment. If you have any questions, get in touch with our team.

TECHNIJIAN
technology as a solution