Microsoft 365 Account Compromise

The Situation

An employee receives an unexpected Microsoft 365 sign-in notification. Shortly afterward, they discover that suspicious emails have been sent from their account.

The business is concerned that the account may have been compromised and that sensitive company information could be at risk.

The Challenge

The business needs to:

- Secure the compromised account
- Prevent unauthorized access
- Determine what happened
- Protect other Microsoft 365 accounts
- Get the employee safely back to work

The Reconnect IT Approach

Reconnect IT can immediately assess the account and Microsoft 365 environment, starting with containment.

We can:

1. Secure the account
Reset credentials, revoke active sessions and review authentication methods.

2. Investigate the activity
Review available sign-in and security information to identify suspicious access and determine the likely source of the compromise.

3. Check for persistence
Look for suspicious inbox rules, forwarding settings, delegated access and other changes an attacker may have made.

4. Strengthen security
Review MFA, conditional access and account security settings and recommend improvements based on the organization's needs.

5. Prevent recurrence
Provide practical recommendations to reduce the likelihood of another account compromise.

The Result

The immediate priority is to regain control of the account and minimize business disruption.

The business also gains a clearer understanding of its Microsoft 365 security posture and the steps needed to better protect its users.

Key Takeaways

- Account secured
- Unauthorized sessions addressed
- Suspicious activity investigated
- Microsoft 365 security reviewed
- Security improvements identified
- Business disruption minimized

The Bottom Line

A compromised Microsoft 365 account can quickly become a business-wide security problem.

If you suspect an account has been compromised, don't wait. Get IT help.