designDATA

IT Made Simple. Modern. Secure.

Getting Better Results Out of Microsoft 365:

Solving Business and Security Challenges by Using What You Already Have

Your email is the most essential major IT system in your organization. Sadly, it's also the most **vulnerable** and **difficult to manage**. Many business and security challenges are introduced through email. Fortunately, Microsoft 365 offers tools that allow your IT, Security, and Compliance teams to tackle these obstacles.

It can be daunting to determine which tool to use when. This quick guide clarifies the most appropriate tools for each business challenge.

Business Challenges:

Microsoft 365 Tools:

Phishing and other malicious emails:
Attachments may contain viruses, insecure links, or gift card scams.

Advanced Threat Protection (ATP):
A security and spam filter for email that provides enterprise-class protection.

Business email compromises:
Attackers can gain access to a user's mailbox and manipulate invoices and transactions.

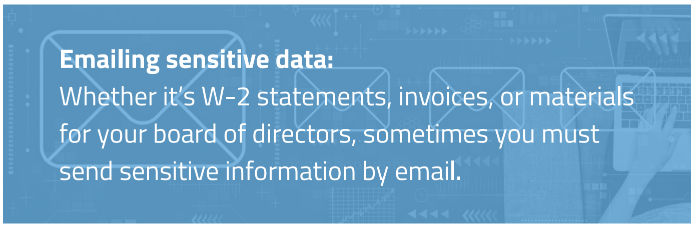
Conditional Access and Security Defaults:
You can manage Multi-Factor Authentication and restrict logins based on geography, time, and source.

Manage business-owned devices:
An increase in remote work means that your team likely doesn't have the tools to manage organization-owned devices.

InTune:
This provides Mobile Device and Mobile Application Management (MDM & MAM). Control the use of your organization's devices and configure specific policies to control applications

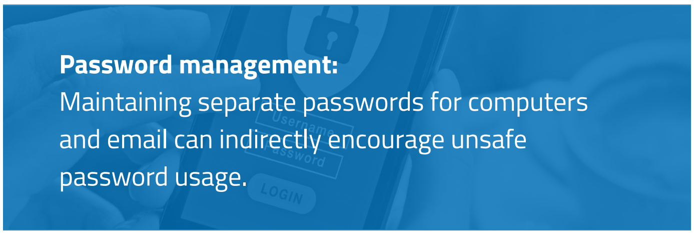
Business email on employee-owned devices:
Organization data co-mingling with employees' personal data makes security breaches more likely. It's also tricky to set restrictions on devices you don't own.

InTune:
Perform remote-wipes of business data if a device is lost or an employee leaves. Restrict copy-and-paste from business to personal apps.



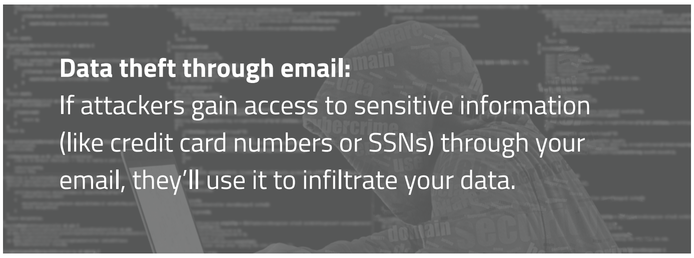
Emailing sensitive data:
Whether it's W-2 statements, invoices, or materials for your board of directors, sometimes you must send sensitive information by email.

Message Encryption:
Encrypt email traffic while in-transit to reduce the risk of snoopers accessing your emails.



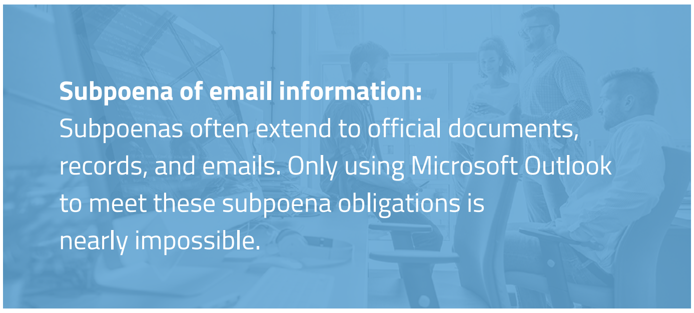
Password management:
Maintaining separate passwords for computers and email can indirectly encourage unsafe password usage.

Password Sync:
Sync passwords from your IT environment (like Active Directory) directly to unify identity management.



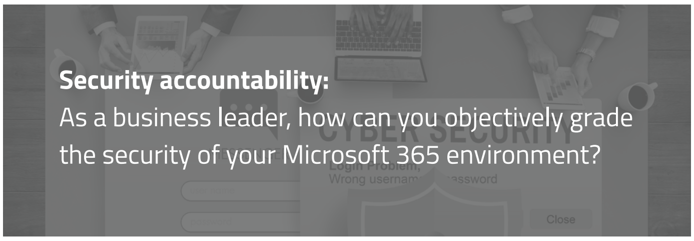
Data theft through email:
If attackers gain access to sensitive information (like credit card numbers or SSNs) through your email, they'll use it to infiltrate your data.

Data Loss Prevention (DLP):
Identify in-transit emails with sensitive data like credit card numbers or SSNs, and either stop them or notify your team.



Subpoena of email information:
Subpoenas often extend to official documents, records, and emails. Only using Microsoft Outlook to meet these subpoena obligations is nearly impossible.

eDiscovery, Legal Hold, and Archiving:
eDiscovery allows your team to search across your entire organization for keywords. Legal Hold prevents emails from being permanently deleted. Archiving maintains older email records without taking up inbox space.



Security accountability:
As a business leader, how can you objectively grade the security of your Microsoft 365 environment?

Microsoft Security Score:
A built-in system to aggregate the security your team has already enabled, score it, and make recommendations for improvement.

With so many business risks born through email, your teams need the right tools to secure your organization. If you need help getting any of these tools implemented, book a free consultation with Microsoft Gold Partner designDATA.

Book a FREE Consultation

designDATA
IT Made Simple. Modern. Secure.

610 Professional Drive, Suite 102, Gaithersburg MD 20879
T: 301-921-6696 **E:** security@designdata.com