Microsoft

Cybersecurity Simplified: BYOD (Bring Your Own Device)

Bring your own device (BYOD) refers to a policy of permitting employees to use personally-owned devices (laptops, tablets, and smartphones) to access company information and applications. BYOD continues to grow in popularity among businesses as a means to increase mobile productivity choices for employees or reduce hardware expenditures.

However, security can be a concern when it comes to BYOD. With an influx of personal devices in the workplace, the possibility of viruses, hacks, and data leaks is elevated. Every device that accesses company information represents an additional endpoint that hackers can attempt to breach.

There are several reasons to offer a BYOD policy:

- **Increased worker satisfaction**. Employees can use the devices they prefer, and enjoy greater productivity because they are using familiar tools.
- **Less IT burden**. Having employees take care of their own device's maintenance means less involvement and work from the information technology's (IT) department.
- **Saving money**. Employees pay for their own devices and the maintenance that goes along with them.
- **Increased employee engagement**. Employees can get work done without having to physically be at the office. This gives them greater flexibility to manage their schedules and stay on top of their work.

What steps can you take to reduce the risks of BYOD?

There are a couple ways to securely offer BYOD:

- Mobile Device Management (MDM), in which the employee enrolls their entire device to allow the security of all data to be managed by the company.
- Mobile Application Management (MAM), allows individual applications to be securely enrolled so only the specific application's data is managed by the company.

Personal devices in the workplace may increase the possibility of viruses, hacks, and data leaks.

Microsoft 365 Business protects company data on your staff's personal devices

Microsoft 365 Business supports both Mobile Device Management and Mobile Application Management, so whichever solution you choose, Microsoft 365 Business can power your BYOD policy. Microsoft 365 Business helps you to securely manage apps and data on iOS, Android and Windows devices.

You can **control which apps are allowed to access company data.** You can require users to access Office 365 from the Office mobile apps and configure policies that keep the data protected (such as encrypting it, protecting it with a PIN, and so on).

You can also **prevent users from moving data to an unsecured app**. You can prevent a user from copying text from their company email and pasting it into an unsecure place, such as their personal email or the Notes app on their phone. You can block a user from saving a spreadsheet of customer data to personal cloud storage (like DropBox, for instance).

You can also **delete company data from a device** if it is lost or stolen, or if an employee leaves the company. And you can do this without impacting personal data from the device. For example, if an employee leaves your company, you can remotely delete all company data from their phone, but their photos, personal contacts, and texts will be untouched.

Why should I use Microsoft 365 Business to support my BYOD policy?

Microsoft Intune – the technology that powers the BYOD environments at many of the world's largest companies – is the technology used by Microsoft 365 Business to support your BYOD policy. Employees can use familiar Office mobile apps instead of 3rd party apps required by other high-security solutions. These capabilities are included with your subscription – there are no additional 3rd party solutions to buy, install, or manage.

Get started:

Learn more about Microsoft 365 Business at www.microsoft.com/microsoft365/business