SMB SECURITY · SECURITY FIELD NOTES

Microsoft 365 Business Premium security for small business: build the floor you own

> *Most business fraud does not start with a clever email you were meant to catch. It starts with a working password. Here is the security floor that stops a valid login from becoming a stolen payment, built from the licences a small firm already holds.*

By **Pedro Bandeira** · 3DH Consulting · Updated August 2026 · 10 min read

Halfway through setting up a new company laptop last week, a firmware update tripped a BitLocker recovery screen. The machine asked for a forty-eight digit key before it would boot

another inch. I had that key. It was sitting in the company's Microsoft tenant, written there automatically the moment the disk encrypted itself. I typed it in, the machine booted, and the build carried on. A boring story, and that is exactly the point. Security that works is boring, and it is almost always something you already own rather than something you bought in a panic.

I put Microsoft 365 to work inside small companies, and I spend most of my time on the part nobody sells you: the floor under the fancy features. Owners ask me which security product to buy. Almost always the honest answer is that they already own the thing that matters, it was just never switched on. This is a plain guide to the security floor a firm of ten to two hundred and fifty people can lay with Microsoft 365 Business Premium, the plan many of them already pay for, and to why that floor stops the attack you are actually facing rather than the one in the brochure.

> ⚠ **THE NUMBER THAT SHOULD WORRY YOU**
>
> In 2024 the FBI's fraud centre logged 2.8 billion dollars lost to business email compromise in a single year, and almost 8.5 billion across the three years to 2024. Almost none of it started with malware. It started with a login that worked. In Verizon's 2025 breach investigation, stolen credentials were the single most common way in, present in 22% of breaches. The lock on your front door is not the problem. Someone is walking in with a copied key.

The attack you are actually facing is a login, not a link

The mental picture most owners carry is a dodgy email with a bad link, the kind you train people to hover over and delete. That threat is real, but it is not where the money goes. Business email compromise is quieter. Someone obtains a valid username and password, for your finance person or for you, logs in from a normal-looking session, reads the mail flow to learn how your company words things, and then sends an invoice change or a payment instruction that looks exactly right. There is nothing to hover over. There is no attachment. It is a legitimate login doing an illegitimate thing.

Where do the credentials come from? Rarely from guessing. They come from reuse, the same password the person also used on a site that got breached. They come from info-stealing malware sitting on a home machine. They come from convincing fakes of your own sign-in page. Verizon's

2025 report found stolen credentials behind 88% of attacks on basic web applications, and company credentials sitting in the logs of 46% of the unmanaged devices it examined, against 30% of managed ones. Read that last pair twice. The device you do not control is half again as likely to be leaking your keys.

This is why the FBI keeps describing business email compromise, in its own words, as the 55 billion dollar scam across the full span it has tracked. The method is not sophisticated. It is patient, and it walks through the one door you left propped open: an identity that can be borrowed.

You cannot train your way out of a valid login

Once an owner understands this, the instinct is to book more security awareness training. Do it, it has its place. But be clear about what it cannot do. Training teaches people to spot the suspicious. A valid login from your finance manager's real account, moving a real-looking invoice to a new account number, is not suspicious. The staff did nothing wrong. There was nothing for them to catch. Awareness is a filter on the front end, and the attack you are facing walks in through the back.

The answer sits lower in the stack, below the human, in how identity and devices are set up. Three controls carry almost the entire load, and a small company already owns all three inside Business Premium. None of them asks an employee to be vigilant on a Tuesday afternoon. They simply make a borrowed key stop working.

> **THE MISTAKE THAT FEELS LIKE SECURITY**
>
> Buying a new security product while the identity basics sit unconfigured is the small-business version of fitting a second deadbolt to a door with the key still under the mat. The spend feels like action. The mat is still there. Configure the floor first, then decide whether you are missing anything above it. Most firms are not.

The floor: three controls you already own

Business Premium is not a light plan. It carries Microsoft Entra ID P1 and Microsoft Intune Plan 1, the identity and device tools that used to be enterprise-only, bundled into the small-business plan. Here is what to switch on, in plain terms and in order.

THE CONTROL	WHAT IT DOES	BUSINESS PREMIUM COMPONENT
Identity you can trust	Stops a borrowed password from signing in	**Entra ID P1, MFA + Conditional Access**
A disk nobody can read	Makes a lost laptop a brick, key held by you	**BitLocker, escrowed via Intune**
A device you can wipe	Clears company data on a machine that walks out	**Intune Plan 1**
An account that cannot self-elevate	Denies malware the admin rights to take the machine	**Standard user + Windows LAPS**

Identity you can trust

Turn on multifactor authentication for everyone, no exceptions, starting with the owner and the finance seats. This one setting does more than every other control combined. Microsoft's own study of account attacks found that multifactor authentication reduces the risk of account compromise by more than 99%, and still blocks the large majority of attacks even when the password has already leaked. Microsoft sees on the order of 600 million identity attacks a day, and more than 99% of them are password-only. Multifactor authentication is the wall those attacks break on.

Then add Conditional Access, the Entra P1 feature that lets you set rules like "no sign-in to mail from outside the countries we work in" or "no access from a device we do not manage." You are narrowing the door from "anyone, anywhere, with the password" to "our people, on our devices, from where we operate." That is the difference between an account that can be borrowed from a basement on another continent and one that cannot.

A disk nobody can read

This is the recovery-screen story from the top of the page. BitLocker encrypts the whole disk, so a laptop that is lost or stolen is useless to whoever finds it, not an open filing cabinet. The part that makes it real for a business, rather than a checkbox, is the escrow. When you deploy it properly, Intune stores the recovery key in your tenant automatically the moment encryption switches on. You, the company, hold the key. Your employee does not have to keep it on a sticky note, and when a firmware update throws a recovery prompt in the middle of a build, the key is one click away instead of a lost day. Encrypting without escrow is how companies lock themselves out of their own machines. The escrow is the whole difference between security and a self-inflicted outage.

A device you can wipe, an account that cannot self-elevate

Enrol the machines in Intune and two more things become true. You can wipe a device remotely if it walks out the door with a leaver or a thief, company data gone without touching the person's own photos. And you can lay the last plank: the everyday account is a standard user, not a local administrator, so a piece of malware that lands in that session cannot quietly promote itself and take the whole machine. The one local admin password that still has to exist is handled by Windows LAPS, which rotates it and stores it in your tenant, so there is no shared admin password on a wiki that every former employee still remembers. Standard-user-by-default is the least glamorous control on this list and one of the most effective, because it turns a single unlucky click into a contained event rather than a company-wide one.

- **Multifactor authentication on, for everyone.**
  Owner and finance first, then the rest the same week. No unprotected exceptions, because the exception becomes the account that gets borrowed.
- **Conditional Access to fence the perimeter.**
  Block legacy authentication that cannot do MFA, restrict sign-in to the countries you actually work from, and prepare the rule that will require a managed device.
- **BitLocker on, key escrowed to the tenant.**
  Prove the recovery path under a real prompt before the machine reaches the user, not after something goes wrong.
- **Enrol every device in Intune.**

This is what makes remote wipe and the compliant-device rule possible at all. It is also the slow part, and it is worth the weeks.

- [ ] **Standard user by default, LAPS on the local admin.**
  Nobody works day to day as an administrator. The single admin account rotates its own password and reports it to the tenant.

- [ ] **Require a compliant device last.**
  Turn on the Conditional Access rule that blocks unmanaged devices only once the fleet is enrolled. Flip it early and you lock out your own people.

The honest part: a floor is laid one plank at a time

Here is what I will not pretend. You do not do all of this on a Tuesday and walk away secure. On that laptop I mentioned, we got the floor right: BitLocker escrowed and proven under a live recovery prompt, Windows LAPS on the local admin, the user set up as a standard user rather than an administrator. One machine, built to standard, verifiable. And the honest next line is that the rest of that company's machines are not there yet. Until they are enrolled, I cannot switch on the Conditional Access rule that blocks logins from unmanaged devices, because right now it would lock out the people still working on the old setup.

That is not a failure of the plan, it is the plan. Security you own is not a product you install in an afternoon, it is a floor you lay one plank at a time, in an order where each plank can bear weight before you stand on the next. The firms that get breached are rarely the ones halfway through laying the floor honestly. They are the ones who bought a shiny alarm, mounted it on the wall, and never checked that the doors underneath it actually locked.

> 📌 **THE ORDER THAT WORKS**
>
> Multifactor authentication everywhere, fence the perimeter with Conditional Access, encrypt and escrow, enrol the devices, drop everyone to standard user, and only then require a managed device. In that order. Every locked-out, angry-staff security rollout I have seen flipped the last rule on first. Lay the planks, then stand on the floor.

What the floor buys you, scenario by scenario

🔑 THE BORROWED PASSWORD

- The finance login leaks in a breach somewhere else
- MFA stops the sign-in cold, no second factor, no entry
- Conditional Access blocks it from an unknown country anyway
- The invoice fraud never gets a session to work with

💻 THE LOST LAPTOP

- A machine is left in a taxi or lifted from a bag
- BitLocker makes the disk unreadable without your key
- You hold the recovery key in the tenant, not the employee
- Remote wipe clears the company data on next contact

🧰 THE RECOVERY PROMPT

- A firmware update trips the BitLocker screen mid-use
- The forty-eight digit key is one click away in your tenant
- No lockout, no lost day, no data held hostage
- The employee never had to keep the key at all

🚪 THE LEAVER

- Someone exits, on good terms or bad
- One action disables their identity across every service
- The device is wiped or reclaimed remotely
- LAPS means no shared admin password walks out with them

The same floor is what everything above it stands on. The identity and device baseline that stops a borrowed login is also the groundwork every compliance duty now assumes you have. It is the starting point of our EU AI Act readiness work, because you cannot govern what your staff feed an AI tool if you do not first control who is logged in and on what device. And it is the same make-it-real-before-you-automate discipline behind our KSeF e-invoicing readiness work: get the boring foundations true, then build on top of them with confidence. Foundations first is never the exciting answer. It is the one that holds.

> **PEDRO'S TAKE**
>
> The small companies that get hurt are almost never the ones without a security budget. They are the ones who spent it in the wrong place, on a product above a floor that was never laid. Business Premium already carries the identity and device controls that stop the

> attack which actually empties bank accounts. Switch on multifactor authentication, fence the perimeter, encrypt and escrow, enrol the devices, and stop everyone working as an administrator. None of it is glamorous. All of it is yours. When the recovery screen shows up, and one day it will, you want to be the one holding the key.

Frequently asked questions

We already have multifactor authentication. Isn't that enough?

It is the single most important control, and it is not the whole floor. MFA stops the borrowed login at the door. It does nothing for the laptop left in a taxi, the disk that can be pulled and read on another machine, or the shared admin password that leaves with an ex-employee. Encryption with escrow, device enrolment, and standard-user accounts cover what MFA cannot. The floor is the set, not one plank.

We are too small to be a target, aren't we?

That belief is a large part of why small firms get hit. Automated attacks do not check your headcount, they check whether a password works. The FBI's fraud losses are dominated by ordinary businesses, not household names, precisely because the small ones assumed they were beneath notice and left the basics switched off. You are not too small. To an automated login attempt you are indistinguishable from anyone else with an unprotected account.

Do we need to buy new security software?

Usually not. If you are on Microsoft 365 Business Premium, you already own Entra ID P1 and Intune Plan 1, the identity and device controls this article describes. The work is configuration, not procurement. The common exception is a firm on a lighter plan, where the fix is a plan change rather than a new product bolted on the side. Spend the money on switching things on, not on buying more.

Not sure your floor is actually laid?

That is the posture review we run. We check what your Microsoft 365 plan already includes, switch on the identity and device controls that stop credential fraud, prove the recovery path before you need it, and hand you the enrolment sequence that gets the whole fleet to standard. It uses the licences you already pay for.

Book a security posture call

Last updated August 2026. This article is for information only and is not security or legal advice. Key sources: the FBI Internet Crime Complaint Center 2024 Annual Report on business email compromise losses (ic3.gov), the Verizon 2025 Data Breach Investigations Report on stolen credentials as an initial access vector (verizon.com), Microsoft Security research on the effectiveness of multifactor authentication (microsoft.com/security), and Microsoft Learn documentation on Microsoft 365 Business Premium security, Intune, and BitLocker (learn.microsoft.com).