LESSON 01 OF 05 · 6 MIN · ESSENTIAL

Why small businesses get hit

It usually isn't personal, and it usually isn't sophisticated. Understanding the economics of an attack makes the fixes obvious.

Opportunistic, not targeted

Most attacks on small businesses are automated. Someone scans the internet for exposed remote desktops, buys a list of leaked email passwords, or sends ten thousand invoices with changed bank details. They don't check your headcount first. They check whether the door opens.

The exceptions are targeted: a supplier impersonation written for your business, a fake IT call that knows your name, a payroll diversion timed for month end. Those use information anyone can find: your website, LinkedIn, an out-of-office reply.

The same five gaps

Across incident after incident, the entry point is familiar:

- An account without **multi-factor authentication**.
- A device or application that hasn't been **updated**.
- A **backup** that was connected, incomplete or never tested.
- Someone who hasn't been shown the **payment and impersonation scams**.
- No **plan** for the first hour, so decisions are made in a panic.

None of those require a security team to fix. They require a few focused hours and someone with the authority to say “we're doing this now”.

Small is an advantage

Large organisations have thousands of devices, legacy systems and committees. You have a handful of laptops, one email platform and the ability to change a

setting this afternoon. That's why a small business can move from “exposed” to “harder than the next business” in a week.

The goal isn't perfect security. It's making the opportunistic attack not worth the effort, and making the targeted one noisy and expensive.

> **THE HONEST BASELINE**
>
> If you do nothing else: MFA on email, automatic updates, one tested offline backup, and a callback rule for bank-detail changes. Those four cover a remarkable amount of real-world risk.

Key takeaways

- ✓ Most attacks are automated and look for common gaps, not important companies.
- ✓ MFA, patching, backups, scam awareness and a first-hour plan cover most of the risk.
- ✓ Being small means you can fix these quickly, use that.