



Digital

Cybersecurity in Schools: A Wake-Up Call from the M&S Attack

The recent cyber-attack on Marks & Spencer has sent a clear message: **no organisation is immune to cybercrime**. If a major, well-resourced retailer can be brought to its knees by a sophisticated breach, what does that mean for schools?

The education sector is increasingly being targeted by cybercriminals. Schools hold a wealth of sensitive data—pupil records, safeguarding information, staff details—that is highly valuable and vulnerable. This data is not just important to your operations; it's precious, and its loss or exposure can have serious consequences.

Why This Matters to Schools

Cyber attacks on schools are becoming more frequent and more damaging. Beyond the immediate disruption, the long-term impact on trust, compliance, and recovery costs can be significant. The M&S incident is a stark reminder that **preparedness is everything**.

Attacks of this scale often lead to a rise in phishing scams and fraudulent activity. That's why it's essential that everyone in your school community—staff, leadership, and even students—understands the risks and knows how to respond.

What Can Schools Do to Stay Protected?

Build a Human Firewall with Cyber Awareness Training

Your staff are your first line of defence. We've partnered with [BoxPhish](#), a Leeds-based cybersecurity training provider, to deliver short, effective training modules designed specifically for schools.

- **Just 5 minutes a month** per module
- **Relevant and jargon-free**
- **Proven to reduce risk and increase awareness**

This training is already helping schools and trusts across the UK build a culture of vigilance. It's a small investment with a big impact.

Ensure You Have Reliable Offsite Backups

When a cyber-attack hits, recovery speed is critical. That's why we work with **Redstor**, whose Remote Backup Service for Schools provides:

- Fully automated, cloud-based backups
- Secure UK-based data centres
- Full compliance with DfE and GDPR requirements

Backups are managed and monitored ensuring:

- Backups run automatically at convenient times
- Daily checks and alerts are actioned promptly
- A full audit trail is available for inspections or incidents

With offsite backups in place, we can help schools recover quickly and minimise disruption—even in the face of a serious breach.

Final Thoughts: Stay Vigilant, Stay Prepared

The M&S cyber-attack is a timely reminder that **cybersecurity is not just an IT issue—it's a whole-school responsibility**. From training your staff to securing your data, every step you take now strengthens your resilience for the future.

If you're unsure where to start, or want to review your current setup, speak to **NYES Digital** or your Relationship Manager. We're here to help you protect what matters most.

nyes.digital@northyorks.gov.uk

01609 536086

nyes@northyorks.gov.uk

01609 533222