MW McEwanWallace By your side

# Cyber Attacks on Retail Giants: What Every Business Should Learn

The recent wave of cyber attacks on UK retailers, including Marks & Spencer, Co-op and Harrods, is a reminder that no organisation is too big - or too prepared - to be targeted. But while the headlines may focus on the big names, there are important lessons here for businesses of all sizes.

The National Cyber Security Centre (NCSC) is working with the affected businesses. In a recent statement they said they are not yet in a position to say if the attacks are linked. However, they are saying that they have insights and there is a lot they do know.

For instance, while not confirming any details, NCSC have commented and provided advice on press speculation that social engineering was used to target IT helpdesks. By impersonating support staff - or posing as employees locked out of their accounts - a hacker might use social engineering tactics to trick people into handing over login credentials and security codes.

It's a disturbingly simple method, but one that works.

The takeaway? People, not just passwords, are your first line of defence.

In its latest guidance, the NCSC urges organisations to review their password reset processes - especially for senior employees who have access to sensitive parts of your network. That means thinking carefully about how identity is verified when someone calls the IT help desk. Is there a secondary check? Would a fraudster be spotted?

Some in the cyber community are even suggesting codewords to help authenticate real users. But that only works if it's part of a broader culture of awareness, where staff are trained to question the unexpected, even if it sounds routine.

### Small businesses aren't immune

While the recent attacks have hit household names, the tactics used don't discriminate by size. If anything, smaller businesses - often without dedicated cyber security teams - can be seen as easier targets. That's why it's essential for you to act now:

- Review how password resets are handled internally. Who has access? What verification steps are in place?

- Use multi-factor authentication wherever possible. A password alone is no longer enough.

- Monitor for unusual logins. Logins from unexpected locations or at odd times should trigger a red flag.

- Recognise social engineering. You and your staff need to know how to recognise potential threats. Making updates regular and having short refresher sessions can go a long way.

## Organised or opportunistic?

The advice from NCSC seems to indicate that these recent incidents are not about high-tech hacking. It’s about gaining trust and then gaining access. This makes it vital to see cyber security not as an IT issue, but a business-wide responsibility.

NCSC have warned that online criminal activity is rampant and attacks like the ones experienced by high profile retailers are becoming more and more common. Businesses of all sizes need to be prepared. The best defence for most organisations starts internally - with stronger processes, clearer communication, and a healthy dose of scepticism.

Now is the time to ask: could this happen to us?

See: https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers