# UK Department for Work and Pensions takes online services offline after cyber incident



The UK's DWP took some online services offline as a precaution after a cyber incident. The nature of the incident is undisclosed, and regular benefit and pension payments are reported as unaffected.

- The DWP said it had an incident and took some online services offline as a precaution.
- The nature of the incident has not been disclosed.
- Regular benefit and pension payments are said to be unaffected.
- The department is working with the NCSC and the Government Cyber Coordination Centre to investigate and restore services.
- The NCSC recently reported a marked rise since September in cyberattacks assisted by AI.

Britain's Department for Work and Pensions (DWP) said on Friday that it had experienced a cyber incident and had taken some of its online services offline as a precaution.

## What is known

The department has not said what kind of incident it was. A spokesperson stated that regular benefit and pension payments are not affected and will continue as normal. The DWP is the largest UK government department by spending and administers the state pension and a range of benefits that millions of people rely on for essential bills.

It said it is working closely with the National Cyber Security Centre and the Government Cyber Coordination Centre to investigate and bring services back as quickly as possible.

## Wider context

The incident follows a statement from the NCSC, days earlier, that it had seen a marked rise since September in cyberattacks assisted by artificial intelligence. Earlier this year the British government also acknowledged that its long-running approach to its own cybersecurity was flawed, said its target of securing all government organisations against known vulnerabilities and attack methods by 2030 could not be met, and described public-sector cyber risk as critically high.

## Why it matters for regulated institutions

The case shows a common response pattern: isolate digital channels first, protect core payment operations, and involve national cyber authorities early. Details are still limited, so no conclusions should be drawn about cause or impact. Institutions that deliver essential services can use the episode to test whether their own containment and communication plans would hold up.

## What to do now

1. Confirm you can take individual digital services offline quickly while keeping core payment and transaction operations running.
2. Review incident response plans for early notification of the NCA and, where applicable, SAMA or other sector regulators.
3. Test customer and public communication templates that explain a precautionary service suspension without disclosing unverified details.
4. Check that business continuity plans define recovery priorities and acceptable downtime for citizen- or customer-facing portals.
5. Include AI-assisted attack scenarios, such as more convincing phishing, in your next threat assessment and awareness material.