Kenneth R. Bagayas

BT-702a

## **Title and Link to the Article**

UK armed forces’ personal data hacked in MoD breach

**Link:** [https://www.theguardian.com/technology/article/2024/may/06/uk-military-personnels-data-hacked-in-mod-payroll-breach](https://www.theguardian.com/technology/article/2024/may/06/uk-military-personnels-data-hacked-in-mod-payroll-breach?utm_source=chatgpt.com)

**Summarize the article in at least seven (7) sentences. Identify whether the attack is active or passive**

The UK Ministry of Defense acknowledged in May 2024 that hackers had taken over a payroll system that handles military personnel's salaries. Sensitive information, including names and bank account numbers, of both active and retired military personnel were made public by the hack; the residences of a smaller group were also hacked. While investigations were underway to ascertain the entire extent of the intrusion, authorities promptly pulled the external contractor's system offline to limit the damage. Because of the possible dangers to military members and their families, the government took the situation seriously even though there was no early indication that the stolen data had been extensively utilized. A helpline and credit monitoring services were made available to those impacted, highlighting the human cost of cyberattacks and how real people's financial and personal security can be abruptly jeopardized.

**Recommendations to Prevent**

**Stricter third-party oversight -** Contractors handling sensitive information must follow the same strict cybersecurity standards as government networks.

**Data encryption** - All sensitive data should be encrypted so that even if accessed, it cannot be misused.

**Early detection systems** - Continuous monitoring should be in place to catch suspicious activity before it leads to a full-scale breach.