

28 July, 2026

Update for partners on WFP's self-registration application (SRA) in Palestine

WFP's self-registration application (SRA) in Palestine is now back online. The updated platform allows users to safely access the application, register, be verified, and update existing information and services. Families do not need to register again. WFP has informed communities about these changes so that all users may access the platform as soon as they are ready to. We are also conducting training for helpdesk staff to address concerns and enquiries from community members.

Key new features in the application include additional identity verification and user authentication steps to improve account security and bolster protection of personal information. The updated application has improved the cyber security controls and validation of the SRA. Detailed and dynamic third-party scans have been conducted, and the overall security posture has been strengthened to ensure the highest level of cyber protection currently available.

Food and cash assistance has continued uninterrupted during this period of strengthening the platform.

Actions taken after the cyber-attack

Following the malicious cyber-attack on the Palestine SRA on May 14th, WFP's cyber security team took immediate action to shut down the platform, contain the intrusion, and strengthen security controls to prevent further exposure.

The platform included the information of 600,000 registered households to receive assistance in Palestine. WFP immediately initiated a corporate cybersecurity review, additional data protection, and a privacy risk assessment. Impacted individuals and stakeholders were notified and a comprehensive independent investigation was launched.

No entity or individual has claimed responsibility. There is no indication that any information has been leaked publicly, nor shared via private forums. The SRA used in Palestine is a corporate system designed, owned, and operated by WFP and no other WFP systems or platforms were impacted.

Cyber-attacks are on the rise

This incident was just the latest example of attacks on humanitarian systems, operations and assets.

Cyber-attacks targeting humanitarian and non-profit organizations have been on the rise. Recent reports indicate the sector is now the second most targeted globally with increasingly sophisticated attacks. WFP maintains a robust defense against daily cyber-attacks on its systems. While completely eliminating the risk of data breaches is impossible, WFP's commitment to security, data protection, and privacy is unwavering. WFP will continue monitoring applications for potential suspicious activity and vulnerabilities while improving cyber security controls and measures, as needed, to defend against illegal and malicious attacks.

Humanitarian systems, data and infrastructure must never be targeted.