FULGAR S.p.A. Strada Casaloldo 55 - 46042 Castel Goffredo (MN) Italy
tel. +39.0376.779900 (r.a.) - fax +39.0376.780850 - info@fulgar.com - www.fulgar.com

Fulgar S.p.A. hereby informs all Employees, Partners, Clients, and Suppliers that, on November 3rd, 2025, the company suffered a cybercriminal attack targeting its IT systems across the national territory.

As a precautionary measure, and in accordance with the company's internal security procedures, all IT systems in Italy were immediately shut down upon identification of the attack.

It is possible that there has been an exfiltration of personal data, although at present such data cannot be individually identified.

The company has promptly established a task force, composed of internal and external professionals, which is currently working to mitigate the impact and restore systems functionality as soon as possible, in cooperation with the competent authorities.

Recommendations

Fulgar S.p.A. urges everyone to exercise heightened caution in relation to any suspicious interactions, both online and offline.

We invite all recipients to review the following informative pages published by the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali):

Phishing – https://www.garanteprivacy.it/temi/cybersecurity/phishing
Vishing – https://www.garanteprivacy.it/temi/cybersecurity/vishing
Smishing – https://www.garanteprivacy.it/temi/cybersecurity/smishing
SIM Swapping – https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9572143

Fraud attempts in such situations can take various forms. Their goal is often to use personal data to extort money and/or obtain additional personal information through fraudulent messages or phone calls, falsely appearing to come from acquaintances or family members, or by attempting to access the victim's personal accounts.

Fulgar S.p.A. strongly recommends that all individuals:

- Carefully evaluate any e-mail, SMS, message, or phone call requesting access codes or other personal data, and verify the legitimacy of the sender. Please note that banks and service providers never request access codes or passwords via SMS, e-mail, or phone calls.

- Be cautious with e-mails, SMS, or other messaging sources containing hyperlinks or unusual attachments, which may be used to redirect users to malicious websites or install malware.

FULGAR S.p.A. Strada Casaloldo 55 - 46042 Castel Goffredo (MN) Italy
tel. +39.0376.779900 (r.a.) - fax +39.0376.780850 - info@fulgar.com - www.fulgar.com

- Change the passwords of all personal accounts (e-mail, social networks, forums, etc.) and, where possible, enable multi-factor authentication (MFA). Multi-factor authentication mechanisms (e.g., OTP codes received from a bank after entering a username and password) enhance protection against unauthorized access. Most major online service providers offer this option, which can be activated in the account security settings.

In case of suspected identity theft, we recommend contacting the Police Authorities.

For any inquiries regarding this cyber-attack or other matters related to data processing, including requests to exercise your data protection rights, please contact:
📧 privacy@fulgar.com