HumanSurface

Exposure Assessment Report

Public exposure analysis focused on phishing, impersonation, and human-targeted fraud.

COMPANY

Rossi Industriali S.r.l.

DOMAIN

rossi-industriali.it

ASSESSMENT DATE

19 March 2026

OVERALL RISK

72 /100

High exposure

Prepared by HumanSurface

Executive Summary

HumanSurface analyzed the public exposure of Rossi Industriali S.r.l. to identify signals that could enable phishing, impersonation, and fraud attempts targeting the organization through people, roles, and business context.

IMPERSONATION RISK	FINANCE FRAUD RISK	HR / SOCIAL ENGINEERING
81	68	74
HIGH	MEDIUM	HIGH

Key takeaways

- Public email addresses were identified on company-related pages.
- Executive and finance-related roles are publicly visible.
- Predictable naming patterns may help attackers guess valid corporate addresses.
- Public business context may support targeted phishing.

Overall conclusion

High risk level

Rossi Industriali shows a high human-surface exposure level, with the strongest immediate risks concentrated around impersonation and finance-related scenarios. Priority actions: reduce public contact exposure, reinforce payment verification, and review public role

Top critical findings

The findings below represent the most immediately actionable exposure signals identified during the assessment.

Public email addresses found on company pages

High

Direct public email exposure increases phishing opportunities and can support impersonation attempts.

Executive visibility exposed

High

Public references to leadership roles increase the credibility of urgent-request fraud and impersonation scenarios.

Predictable naming pattern detected

Medium

Visible patterns may allow attackers to guess additional valid corporate addresses.

Public HR-related contact exposure

Medium

Visible HR contacts may attract malicious candidate outreach or targeted social engineering attempts.

People and roles most at risk

Laura Bianchi - CFO	84	Payment fraud
Marco Rossi - CEO	81	Executive impersonation
Giulia Verdi - HR Manager	76	Fake candidate phishing

Plausible attack scenarios

Executive impersonation request

Probability: High - Impact: High

An attacker could impersonate a visible executive and send an urgent internal-looking request to finance or operations, relying on public role visibility and organizational context.

Finance-targeted payment fraud

Probability: Medium - Impact: High

An attacker could target finance-related contacts with a spoofed payment update, invoice change, or supplier-related request.

Immediate remediation

Reduce public email exposure
High priority

Introduce payment verification controls
High priority

Train finance and HR teams
High priority

Review public team pages
Medium priority

Strengthen anti-spoofing controls
High priority

What changed in the last 7 days

Recent changes indicate increased public exposure, mainly driven by additional public contact visibility.

7-day delta

- +2 public email addresses detected
- +1 HR-related public contact page discovered
- HumanSurface Score increased from 64 to 72
- Executive visibility unchanged
- Finance-related exposure unchanged

Recommended next step

Start ongoing monitoring to detect meaningful changes in exposure over time and maintain visibility across executive, finance, and HR-related risks.

humansurface@soreya.app soreya.app

Final assessment

HumanSurface identified a meaningful level of public exposure that could support phishing, impersonation, and fraud attempts against the organization.