Fable

Prepare your firm for Silent Ransom Group's tactics.

Create targeted training, test employees with realistic voice simulations, and identify where your firm needs additional reinforcement.

Silent Ransom Group targets law firms by impersonating IT support, persuading employees to grant access, and stealing confidential information for extortion.

A costly, fast-moving threat to law firms.

IT IMPERSONATION → REQUEST FOR ACCESS → DATA THEFT AND EXTORTION

$46M+

Reported extortion payments across three major U.S. law firms. [1]

REPORTED AUGUST 2026

70%+

Of observed victims were U.S. law firms, according to S-RM's July 2026 analysis. [3]

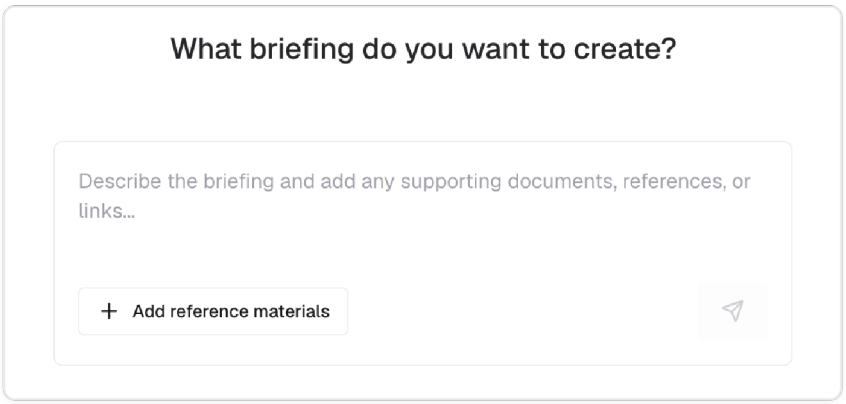
Extortion in a day

From initial contact to data theft and extortion within one business day, in many incidents investigated by Mandiant. [2]

1 Turn an emerging threat into training your people can use.

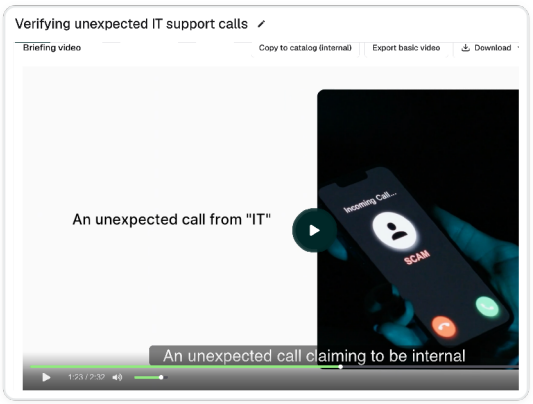
Create a custom briefing that teaches attorneys and staff how to recognize suspicious IT requests, verify the caller through an approved channel, and report concerns using your firm's process.

01 DESCRIBE THE THREAT



Create training on fake IT calls, tailored to your firm's verification and reporting procedures.

02 PREPARE YOUR WORKFORCE

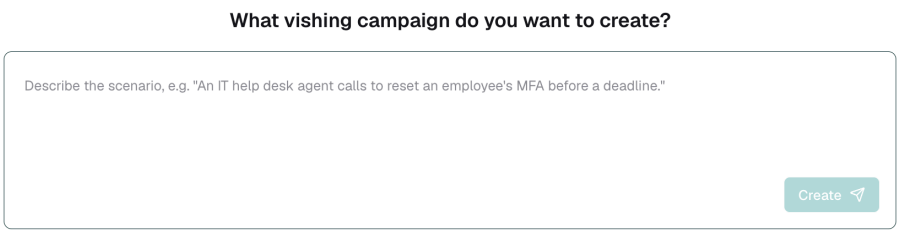


A custom briefing video, ready for your staff to watch.

2 Test how employees respond when "IT" calls.

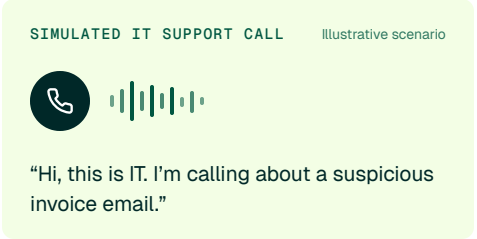
Build a voice-phishing simulation inspired by Silent Ransom Group's tactics. Customize the caller's persona, pretext, and objective to test employee responses and uncover remaining exposure.

01 DESCRIBE THE SCENARIO



Describe the caller, pretext, and objective in plain language.

02 TEST EMPLOYEE RESPONSE



Test whether employees recognize impersonation and verify the request.

Prepare employees. Test readiness. Focus follow-up where it matters.

See Fable in action →

Threat source: FBI, Silent Ransom Group Impersonating IT Personnel through Social Engineering, May 26, 2026. Screens show product creation and configuration; the call artwork is illustrative.

[1] The Insurer, August 7, 2026. Reported payments across Weil Gotshal, WilmerHale, and Goodwin Procter, citing people familiar with the matters. Payment amounts have not been publicly confirmed by the firms.

[2] Mandiant / Google Threat Intelligence Group, June 5, 2026, "Seeking Counsel: Ongoing Targeted Campaign Against US Law Firms."

[3] S-RM, July 2, 2026, "Ransomware in focus: Luna Moth." Analysis describes targeting since 2024.