

Phishing Security Test Report

Campaign: **Security Awareness Wave 1** | Generated on: 2026-09-04 13:15:46 IST

Executive Summary

Overall Risk Score

HIGH

Phishing Risk Level

CAPS Risk Score

80%

Amplified Penalty Weighting Model

F

Risk Grade

0:1

Resiliency Ratio (reported-safe per compromised)

🚩 **Most Vulnerable Department**
IT — **81% risk** (8 credentials, 7 attachment opens, 4 media grants, 9 clicks, out of 9 targeted users)

Campaign Objectives & Findings

- **Engagement:** 15 emails opened, with 14 users clicking the link.
- **Reporting:** 0 users actively reported the email as a threat.
- **Data Exposure:** Captured 3 webcam images and 3 location pings.
- **Credential Risk:** 13 users submitted credentials.
- **Attachment Risk:** 12 users downloaded/opened the simulated attachment.
- **Near Misses:** 1 users opened the email but did not click.
- **AI Retargeting Effectiveness:** Initial templates converted at 93.3%, while personalized AI templates converted at 100%.
- **Training Gap:** 10 compromised users have no completed training assigned yet — an immediate remediation list.

Advanced Threat Metrics

92.9%

Landing Page Conversion
Credentials ÷ Clicked

1

Near Misses
Opened but did not click

0

Ghost Segment
Received, never opened

1h 19m

Avg. Time-to-Click
SOC Window before response

2m

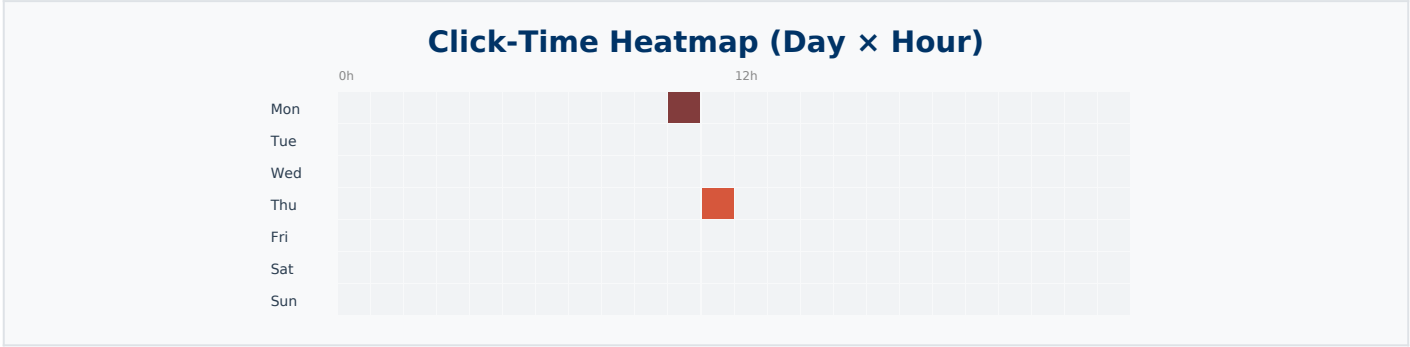
Avg. Dwell Time
Click to credentials submit

3

Triple Threat Users
Click + Creds + Media

Behavioral Trajectory & Temporal Risk

Behavioral Outcomes	Temporal Vulnerability
• Repeat Offenders: 1 (Failed Initial AND Retarget) • Resilient Users: 0 (Failed Initial, ignored Retarget) • Escalated Threat: 0 (Riskier action taken in Phase 2) • De-escalated: 1 (Failed P1, but safer in Phase 2)	• Peak Vulnerable Window: Monday, 10:00 - 11:00 (see click-time heatmap below) • Average Dwell Time: 2m (Time spent on malicious landing page)



Department Risk Breakdown

Department	Users	Sent	Participation %	Opened	Clicked	Credentials	Media	Attachment	Risk %
IT	9	9	100%	9	9	8	4	7	81%
Finance	6	6	100%	6	5	5	2	5	79%

Template Performance

Phase	Template	Sent	Opened	Clicked	Credentials	Click Rate %
AI Retarget	Facebook Login	1	1	1	1	100%
Initial	Microsoft-Security-Alert	15	15	14	13	93.3%

Click Rate reflects the template actually recorded per send — accurate under shuffle mode, where the campaign's configured template pool doesn't map 1:1 to any single recipient.

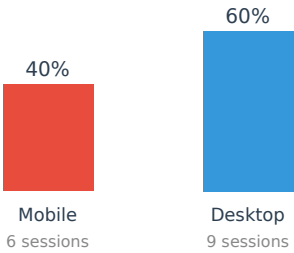
AI Engine Pipeline & Efficacy

Decisions Evaluated	Retarget Emails Sent	Phase 1 Conversion	Phase 2 (AI) Conversion
14	1	93.3%	100%

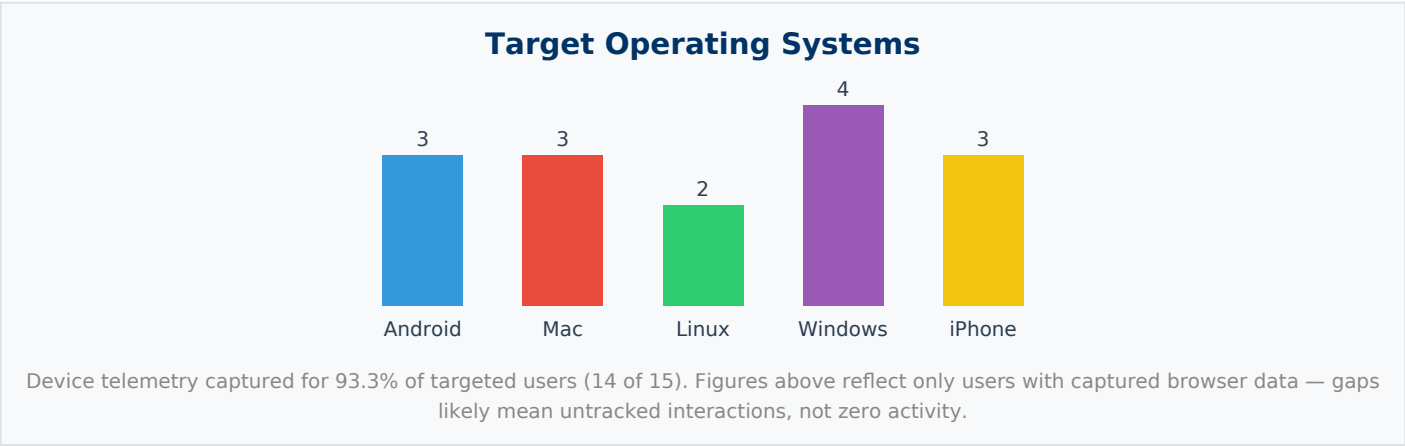
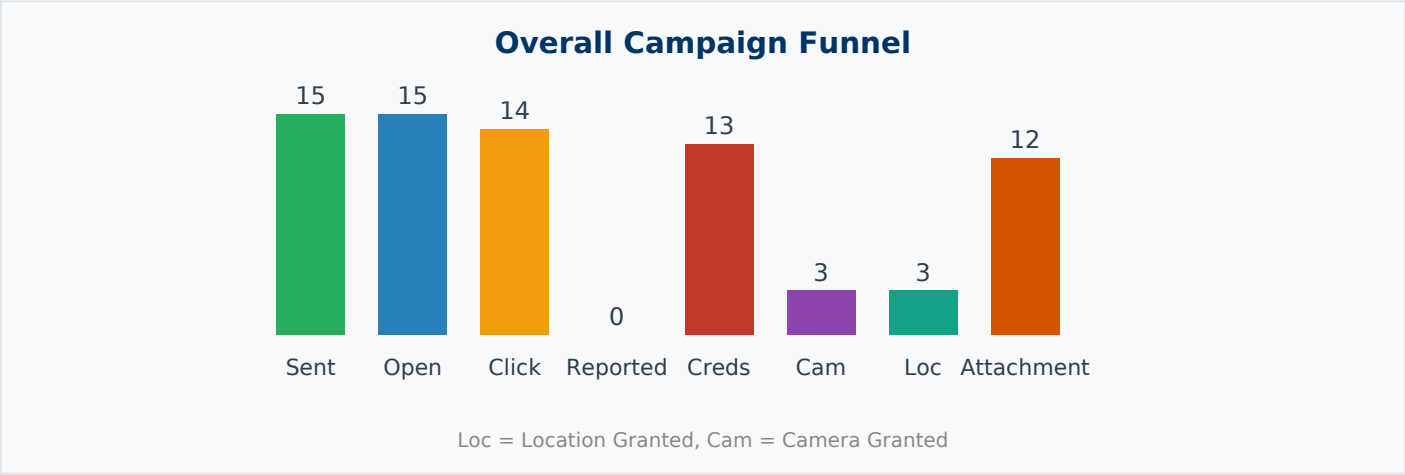
Interaction Sessions by Environment

Environment	Total Sessions	Percentage
Mobile	6	40%
Desktop	9	60%

Interactions are 1.5x more likely to occur on Desktop.



Performance Breakdown Charts



User Activity Summary

How "Final Status" is determined

Each recipient's Final Status is the single highest-priority stage they reached, across both the initial send and any AI retarget: **Not Sent** → **Queued** → **Email Sent** → **Email Opened** → **Link Clicked** → **Location Granted** → **Camera Granted** → **Credentials Submitted** → **Attachment Opened**. Later stages in this list outrank earlier ones regardless of order reached, so a user who clicked and then submitted credentials shows "Credentials Submitted," not "Link Clicked."

S.No	Name	Email	Department	Final Status	Compromised	Reported
1	Priya Nair	priya.nair@capsplatform-demo.com	Finance	Attachment Opened	Yes	No

S.No	Name	Email	Department	Final Status	Compromised	Reported
2	Rohan Verma	rohan.verma@capsplatform-demo.com	Finance	Attachment Opened	Yes	No
3	Meera Iyer	meera.iyer@capsplatform-demo.com	Finance	Attachment Opened	Yes	No
4	Arjun Kapoor	arjun.kapoor@capsplatform-demo.com	Finance	Attachment Opened	Yes	No
5	Vikram Desai	vikram.desai@capsplatform-demo.com	Finance	Attachment Opened	Yes	No
6	Karan Mehta	karan.mehta@capsplatform-demo.com	IT	Attachment Opened	Yes	No
7	Ananya Bose	ananya.bose@capsplatform-demo.com	IT	Attachment Opened	Yes	No
8	Rahul Chatterjee	rahul.chatterjee@capsplatform-demo.com	IT	Attachment Opened	Yes	No
9	Divya Menon	divya.menon@capsplatform-demo.com	IT	Attachment Opened	Yes	No
10	Siddharth Joshi	siddharth.joshi@capsplatform-demo.com	IT	Attachment Opened	Yes	No
11	Neha Pillai	neha.pillai@capsplatform-demo.com	IT	Attachment Opened	Yes	No
12	Aditya Ghosh	aditya.ghosh@capsplatform-demo.com	IT	Attachment Opened	Yes	No
13	Kavya Reddy	kavya.reddy@capsplatform-demo.com	IT	Credentials Submitted	Yes	No
14	Manish Trivedi	manish.trivedi@capsplatform-demo.com	IT	Link Clicked	Yes	No
15	Sneha Rao	sneha.rao@capsplatform-demo.com	Finance	Email Opened	No	No

Recommendations

Long-Term Strategy

- Implement mandatory, ongoing security awareness training for all employees.
- Continue with quarterly phishing simulations to benchmark improvements and adapt to evolving threats.
- Establish SOC email-pull SLA based on the average Time-to-Click (1h 19m).
- Review and restrict browser permissions (camera, location) on all corporate-managed devices.