

Keywords: anti-phishing;e-mail;identity; BEC;
evaluation; assessment; testing; test plan;

March 22nd, 2026
AMTSO Publication: March 23rd, 2026

Version 1.1



Email Phishing & BEC Evaluation H1 2026

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. (“AMTSO”) Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the “Standard”). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.4]. Artifact Security is solely responsible for the content of this Test Plan.

Table of Contents

1. Introduction	3
2. Scope	3
3. Methodology and Strategy	3
4. Participation	4
5. Environment	4
6. Schedule	4
7. Control Procedures	5
8. Dependencies	5
9. Scoring Process	5
10. Dispute Process	5
11. Attestations	5

Email Phishing & BEC Test Plan H1 2026

1. Introduction

This Test Plan was developed in concert with the AMTSO Testing Protocol Standards to support Artifact Security’s Email Phishing & BEC Evaluation submission test for AMTSO accreditation. Artifact Security aims to follow the AMTSO Testing Protocol standard throughout the operation of the test and publication of results.

2. Scope

This evaluation aims to measure the effectiveness of email security solutions when defending against Phishing & Business Email Compromise (BEC). The secondary goal is to evaluate Remediation Capabilities, measuring how effectively a solution can contain a threat after delivery, identify account takeovers and roll back malicious configuration changes

Product Vendor	Product Name
DarkTrace	Email Security
Barracuda	Email Protection
Checkpoint	Email Security
Microsoft	Microsoft 365 E5
Google	Workspace Enterprise Plus

Attack types:

- BEC
- Phishing

The corpus is made of crafted attacks designed and validated by Artifact Security

3. Methodology and Strategy

Detailed methodology can be found on Artifact Security [website](#) and Artifact Transparency [Portal](#). The evaluation covers whole solutions that tackle Email & Identity Security. Target infrastructure is hosted on standard Office 365 Basic.

4. Participation

Opt-Out Policy: Vendors may choose to opt-out based on technical limitation of report publication via info@artifactsecurity.co.uk. Public commentary is allowed on completion of report.

Conflict of Interest Disclosure: no conflicts of interests have been identified.

Funding: The test is self-funded by Artifact Security, usage of report, awards or troubleshooting services for the purposes of product improvement can be purchased. Test result validation is free of charge.

5. Environment

Physical Configuration: The test environment consists of Target Identities reflecting relationships built in a target organisation.

Sample Relevance: Scenarios in this test are based on Business Email Compromise (BEC) and Targeted Phishing based on the latest techniques available via open source threat intelligence

Geographic Limitations: Test Scenarios are focused on English language samples. Main target audience is Europe and North America.

Curation Process: Scenarios contain only crafted attacks based on current threat intelligence. All malicious scenarios used contain clear malicious intent. Participant vendors may provide feedback on the curation process which may lead to scenario exclusion prior to publication.

Distribution of Test Data: All collected test data such as scenario detail, traffic captures (where applicable), product logs and other test artifacts can be shared with participants upon completion of the test scenario.

6. Schedule

Schedule Summary for Test Project

Index	Test Activity	Date(s)	Dependencies
1	Vendor Selection End	03 April 2026	
2	Deployment	06-10 April 2026	
3	Baselining	13-24 April 2026	
4	Testing Phase	29 April - 14 May 2026	(2, 3)
5	Feedback and Dispute Phase	18-29 May	(4)

Communications: Artifact Security will make best effort to notify participants of major delays from the above schedule or any major issues occurring during the test.

Risks and Risk Management: No significant risk has been identified to execution and delivery of the test.

7. Control Procedures

The Test Plan may include instructions for potential Participants to provide Specific Data regarding the Product(s) to be included in the test. These elements are included in the Control Procedures section.

Connectivity Validation: Each product has unfiltered access to the internet throughout the test.

Logging: Instructions for enabling logging within the Product must be provided by the Participant upon request before the 10th April 2026. Any specific logging can be requested via email at stefan@artifactsecurity.co.uk

Updates: The tested solutions are cloud based solutions with unfiltered internet connectivity. Updates are allowed throughout the test and will be reflected in the final report.

8. Dependencies

Participant and Test Subject Vendors Required Actions: Participant status can be confirmed via contacting stefan@artifactsecurity.co.uk or info@artifactsecurity.co.uk

9. Scoring Process

Detailed scoring process is available on the test methodology [here](#).

10. Dispute Process

Preliminary results will be shared with security vendor contact, this includes complete scoring spreadsheet, tested scenario details, product logs & any other test artifacts relevant.

Evidence Sharing Policy: Result validation is provided free of charge to all participants.

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to “I” or “me” or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)
 2. All products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)
 3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test. (Section 2, Section 3)
 4. Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards. (Section 4)
 5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)
 6. I will disclose how the Test was funded. (Section 4)
- I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature:

Name: Stefan Dumitrascu

Test Lab: Artifact Security

AMTSO Test ID: AMTSO-LS1-TP194