Playbook

Human Risk Management for Phishing/Whaling

This comprehensive playbook addresses the evolving threat landscape of targeted phishing attacks, incorporating AI-driven attack vectors, and sophisticated social engineering tactics. This playbook provides guidance on mitigating risks associated with users who are targeted by phishing and whaling attacks. Use this playbook to design and implement controls, policies, and workflows appropriate for your environment and risk tolerance.

Note: This playbook is designed to work across Mimecast Email Security Cloud Gateway, Incydr and Engage – depending on the tools you have deployed you may be able to match functionality in your insider risk/DLP and Awareness training solutions.

Table of Contents

1. Risk Scenarios and Business Impact

Scenario summary

Users face targeting through sophisticated phishing and whaling campaigns that leverage artificial intelligence and multi-channel attack vectors. These attacks have evolved beyond traditional email phishing to include AI-generated personalized messages, impersonation, and coordinated multi-platform social engineering campaigns targeting C-suite executives and senior leadership teams.

Attackers exploit publicly available information, breached credentials, and social media data to craft hyper-personalized messages that mimic executive communication styles and attempt to bypass traditional security controls.

Business impact

Phishing and whaling attacks can lead to severe consequences, including:

- Data breaches and loss of sensitive information
- Financial fraud or unauthorized transactions
- Compliance violations (e.g., GDPR, HIPAA)
- Reputational damage to the organization
- Operational disruptions due to compromised accounts

Supporting policies, compliance, best practices, or governance

- Policies requiring multi-factor authentication (MFA) for all users
- Email security best practices, such as URL and attachment scanning
- Compliance with ISO 27001, NIST CSF, and other relevant frameworks
- Governance policies mandating regular phishing simulations and training

2. Targeted Security Outcomes

High-Level Control Objectives for Phishing/Whaling Scenarios:

- ***Increase awareness:*** Educate users on identifying phishing and whaling attempts.
- ***Strengthen defenses:*** Implement advanced email security measures to block malicious emails.
- ***Encourage proactive behavior:*** Nudge users to report suspicious emails and follow secure practices.

Key outcomes

- Reduce the likelihood of users falling victim to phishing attacks.
- Minimize the impact of successful phishing attempts through rapid detection and response.
- Foster a culture of security awareness and vigilance.

3. Control Strategy and Phased Implementation

Mimecast recommends a targeted and phased approach whenever implementing controls that impact users and user productivity. The following outlines how Mimecast email security, Engage and Incydr policies can be applied in a graduated manner to address the risk of phishing/whaling attacks, especially for high-risk users.

Note: A user's attack factor decreases over time based on sustained reduction in threats from across email and identity, following a rolling 30-day average of the user's intermediate score, which is a comparison of how attacked that user is compared to their peers. This approach ensures that risk-based controls like enhanced filtering, access restrictions, or additional authentication requirements can be relaxed as users are less attacked to their peers, creating dynamic security postures that respond to actual current risk rather than maintaining static penalties based on historical incidents.

Phase 1: Visibility

Objective Start by monitoring.

- Enable alerting for phishing-related activities (e.g., clicking on malicious links, opening suspicious attachments).
- Deploy phishing simulations to assess user susceptibility and identify high-risk individuals.
- Provide real-time feedback to users during simulations to reinforce learning.
- Track which users report phishing attacks and provide education on proper reporting procedures to those who do not report.

Apply visual cues

- Email tagging or warning banners: Mimecast can add splash pages for links that are suspected of being phishing attempts, alerting users without blocking actions.

Begin communications

- Consider sending notifications to the affected users to advise them of the specific attacks targeting them.
- Set expectations and educate users about phishing risks and reporting procedures. Mimecast has curated a set of end user assets to aid in the enablement of end users.

Reference knowledgebase articles:

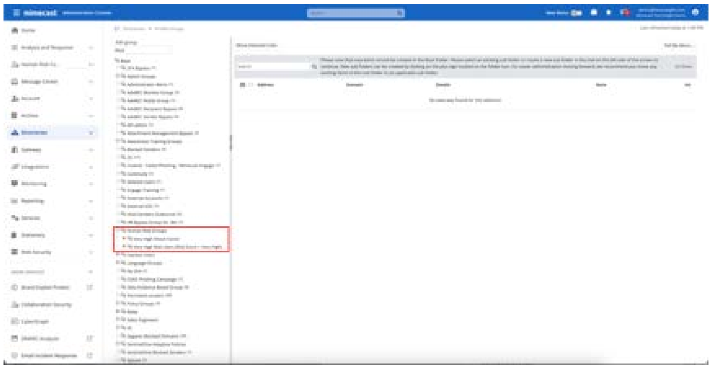
- [Cybergraph - How to add inline banners]
- [Impersonation Protect - How to add inline banners]

Phase 2: Hard Controls

Objective Enforce high-confidence controls for attack scenarios.

Policy-based escalation

- ***Auto-escalate based on thresholds:*** Users who are frequently targeted by phishing and malware attacks, can be moved to stricter policy groups in both Mimecast and Incydr, increasing the security of their accounts and reducing the likelihood of compromise. The profile groups utilized in this scenario is called 'Very High Attack Factor'.



Email Security Attachment Scanning

Prevent the delivery of malicious attachments and ensure comprehensive scanning of all email traffic through Attachment Protect policy set for on-demand analysis with safe file backup enabled.

- Set any fallback action “Hold for Admin Review” to ensure suspicious attachments require manual approval before delivery.
- Enable scanning for both inbound and internal message flows to prevent lateral movement and ensure comprehensive coverage.
- Remove the users ability to edit attachments received from external recipients

Email Security Link Scanning

Mitigate risks from malicious URLs and prevent credential theft through aggressive URL category scanning – this results in anything resembling a URL pattern, including IP addresses and internal links being scanned.

- Enable browser isolation policies to prevent text extraction and credential theft by executing web content in a remote environment.

Email Security Spam Scanning

Enhance spam detection sensitivity while maintaining legitimate message flow. by setting detection engines “Aggressive”.

- Create any bypass rules for trusted senders as needed.

Email Security Impersonation Attempts

Detect and mitigate impersonation attempts targeting high-risk users. through a two-tier policy structure:

- ***First Policy:*** Tag subject lines and message bodies when two impersonation indicators are detected.
- ***Second Policy:*** Automatically hold messages for administrative evaluation when three or more detection hits are identified.

Email Security Business Email Compromise

Protect against Business Email Compromise (BEC) attacks with tailored enforcement levels consisting of:

- Moderate Enforcement: General threat detection across all users.
- Sender Bypass Rules: For verified trusted sources.
- Recipient Bypass Controls: For internal communications.
- Deploy an Aggressive ABEC Policy specifically targeting high-risk individuals who face elevated threat exposure.

Data Exfiltration

Highly attacked users may be utilized as an exfiltration point on a compromised account. Increased monitoring is recommended as an event may happen based on the likelihood of a successful attack.

Awareness Training

Increasing awareness training frequency and targeting content to users’ specific attack vectors significantly improves threat recognition and defensive behaviors by leveraging spaced repetition principles and reinforce security decision-making.

Identity and Access Management (performed through Mimecast ecosystem partners)

- ***Implement tiered password reset based on user risk profiles:*** Low attacked users who demonstrate consistent, normal attack patterns receive immediate access to self-service password reset portals with standard verification. Users flagged as highly attacked are directed to live helpdesk agents who perform enhanced identity verification before processing any account changes.
- ***Increase MFA setting:*** Adjust MFA security controls to be more restrictive, especially for high value corporate resources.
- ***Proactive Access review:*** Initiate access review process for access and permissions to remove unnecessary/unneeded permissions.

Integration Note: Mimecast and Incydr can be integrated to synchronize user profile groups and watch lists, ensuring that high-risk users identified in one platform are automatically reflected in the other. This enables a unified, dynamic approach to human risk management, with graduated policy responses that scale from gentle guidance to comprehensive access restrictions.

General Notes for All Policies

Testing and Pilot Deployment:

- It is best to test each policy in a pilot group before full deployment.
- Follow your organizations change control process for implementation of policy changes.
- Monitor dashboards in the Mimecast AdCon to track effectiveness and administrative overhead.

Optimization Period:

- Policy optimization typically requires 2-4 weeks of operational data to fine-tune detection parameters and minimize false positives while maintaining security efficacy.

Reference knowledgebase articles

- [Email Security Attachment Protection]
- [Email Security Spam Scanning]
- [Email Security Impersonation Protection]
- [Email Security Advanced BEC Protection]
- [Email Security URL Protection]
- [Integrating Mimecast Email Security and Incydr]
- [Incydr Watchlists]
- [Automated Profile Group Assignment]
- [Targeted Awareness Training in Engage]

4. Stakeholder Engagement and Enablement

How to get people aligned, why this is important and how to approach it (from the perspective of the IT or Security practitioner)

Executive Leadership Team (ELT)

- Advocate for phishing prevention initiatives and allocate resources.
- Approve risk tolerance levels and policy directions.
- Monitor progress through regular updates and metrics.

Security Operations

- Design and implement phishing detection and prevention measures.
- Monitor email traffic for signs of phishing and respond to incidents.
- Coordinate with IT and other teams for seamless integration of controls.

IT / Infrastructure Teams

- Support the deployment of email security tools and policies.
- Ensure proper configuration of email gateways and identity systems.
- Maintain the availability and reliability of security infrastructure.

5. Response and Operational Support

What to do when the control triggers or alert fires.

Detection Logic / Alert Criteria

Alerts Triggered by:

- Phishing emails, both delivered and blocked, targeting an individual.
- Attempted malware executions (via External EDR Integration)
- Suspicious login activity like impossible travel or brute force attempts (via external Identity integration)

Response Playbook

1. ***Validate Alert:*** Review the email and user activity to confirm the phishing attempt
2. ***Contain Threat:***
   - Quarantine the email and block further communication with the malicious sender.
   - Reset the user's credentials if necessary.
3. ***Educate User:*** Notify the user of the incident and provide immediate training or guidance.
4. ***Document Incident:*** Log the event in the ticketing system or SOAR platform for tracking and analysis.

Notes

- Export alerts to XDR/SIEM or SOAR for centralized monitoring and triage/investigation.
- Integrate with HR systems to notify managers of incidents involving their team members.
- Trigger legal or compliance reviews for incidents involving sensitive roles.

6. Continuous Improvement and Effectiveness Measurement

Effectiveness Metrics

- Reduction in the percentage of users clicking on phishing links over time.
- Decrease in the number of successful phishing incidents.
- Improved detection rates for phishing emails.

User Engagement Metrics

- Percentage of users completing phishing awareness training.
- Number of phishing emails reported by users.
- Feedback from users on the effectiveness of training and controls.

Governance & Compliance

- Conduct quarterly reviews of phishing policies and controls.
- Align with compliance requirements (e.g., ISO 27001, NIST CSF).
- Provide regular reports to the executive leadership team and risk committees.

Profile Group Reference Guide

Making use of Groups in Mimecast

While seeming simple, groups provide the ability to heavily alter how Mimecast functions, and how a user's interaction with Mimecast can be changed.

Mail flow

Mail flow actions are organized in proactive and reactive groups:

- ***Proactive groups*** are commonly professional service organizations and financial institutions, where protecting intellectual property, finances and reputation are key factors.
- ***Reactive groups*** are commonly healthcare, where failure to communicate timely could affect the well-being of a person.

Outbound and Internal

Proactive Actions			
Actions	**Example**	**Prevention Type**	**More Information**
Block a user from sending to the customer's top-10 client or vendor group	High-risk user is not able to represent the company	Supply-chain attack, Insider threat	Using a group that contains a high-risk user and another group that contains the "Top-10" list, a Blocked Sender Policy can be created to prevent the first group from communicating with the second group
Block a user from sending any email outbound	User is not able to use email as a point of data-exfiltration to their personal account	Insider threat, Potential leaver	A Blocked Sender Policy can be applied using the group
More strict scanning is applied to URLs (e.g., questionable, but not outright malicious) in all outbound email from a user, to identify attempted supply-chain attack or insider threat	High-risk user is not able to send a link to a domain similar to their own or a client's domain	Supply-chain attack, Insider threat	An alternate URL Protection Policy can be applied
Prevent a user from being allowed to send specific attachment types, regardless of their scan results	High-risk user is not allowed to send out zipped or password-protected zip files	Supply-chain attack, Insider threat, Potential leaver	An alternate Attachment Management Policy can be applied
Hold all outbound emails for a user	High-risk user is not able to represent the company at all, and messages must be reviewed before going out	Supply-chain attack, Insider threat	A Content Examination Policy can be applied, using the hold action
Flag or hold a user's outbound messages which contain some less confident phrases indicating supply-chain attack or insider threat	High-risk user is not able to send emails with phrases or words of urgency sent outbound, and generate an alert if internal	Supply-chain attack, Insider threat	A Content Examination Policy can be applied, using the hold action
A user's ability to send outbound emails can be throttled altogether, or based on specific patterns in the message	High-risk user is not allowed to send emails at a pace that could resemble a spray-and-pray attack	Supply-chain attack, Insider threat, Potential leaver	A Recipient Limitation Policy can be applied

Reactive Actions

Actions	Example	More Information
Outbound messages can be sent as Secure Messages, where we retain chain of custody and can revoke access to those message after-the-fact	High-Risk user's outbound emails can effectively be 'recalled' regardless of the recipient's mail platform	A Secure Messaging Policy can be applied
All User's outbound and internal messages are copied to a security team for manual review	High-risk user's messages are BCC'd to a mailbox for review	A Group Carbon Copy Policy can be applied
User's outbound and internal messages matching specific words or phrases alert a security team for review	High-risk user's messages containing words or phrases of urgency are BCC'd to security mailbox for review	A Content Examination Policy can be applied, with the Group Carbon Copy action
Alerts are generated for any lower-confidence scan on outbound emails	High-risk user sending PDF, Office or zip files outbound alert the security team	An alternate Attachment Management Policy can be applied
Outbound emails have a banner applied indicating that the sender's communication should be confirmed via a known alternative communication method	High-risk user's outbound emails have a "Does this communication seem out of the ordinary? Please call our main office and ask to be transferred to this user for verification." banner applied	A Stationery Policy can be applied

Inbound

Proactive Actions

Actions	Example	More Information
Low-confidence phishing emails are administratively held for high-risk users, where they would have been otherwise held at a user level or had a banner apply	High-risk user cannot receive emails with only one or two suspicious indicators	An Impersonation Protection policy can be applied, using the Hold action at an administrative level
Remove some of all attachments from emails, regardless of their scan result	High-risk user is not allowed to receive password-protected zip files that cannot be brute-forced for scanning by Mimecast	An alternate Attachment Management Policy can be applied
Apply more strict URL scanning	High-risk user is not allowed to click on links in a message that are similar to the top-10 vendor/client domains	An alternate URL Protection Policy can be applied

Reactive Actions

Actions	Example	More Information
Smart tags can be applied where recipient is a high-risk user and the message contains low-confidence indicators	Messages to a high-risk user with words or phrases of urgency are flagged for review out-of-band	A Smart Tag Assignment Policy can be applied
Low-confidence phishing emails to high-risk users generate an alert	Security team is alerted with a high-risk user receives an email that matched only a single phrase	An Impersonation Protection Policy can be applied, with the notification option configured
Apply more strict URL scanning	High-risk user is not allowed to click on links in a message that are similar to the top-10 vendor/client domains	An alternate URL Protection Policy can be applied

Interaction

Access to Mimecast

Users added to a group can have a reduced experience, removing access to features like:

Feature	Information	More Information
Searching the archive	We retain up to 99 years of customers' emails outside M365 and Google Workspace, which may contain company confidential or proprietary information	An alternate Application Setting can be applied, with search options restricted to disabled
Sending or receiving emails through Mimecast (as an alternative to M365 or Google Workspace)	Mimecast have a continuity product, where a customer can continue to send/ receive through Mimecast in the event of an issue accessing M365 or Google Workspace	An alternate Application Setting can be applied, with the option to send emails disabled

Access Restrictions

Access restrictions can be applied, such as:

Restriction	Example	More Information
Restrict access based on IP ranges	Access to Mimecast's archive, continuity, and hold queues can be restricted to physical office locations for potentially compromised users	An alternate Application Setting can be applied, which uses an alternate Authentication Profile
Restrict access to web, mobile apps, Outlook plugin altogether or individually	High-risk users are unable to use Mimecast's mobile app to send/receive email	An alternate Application Setting can be applied, which has specific or all methods of accessing Mimecast disabled
Remove the ability to manage held queue items	High-risk user cannot be trusted to release messages held by Mimecast as spam or graymail (also known as bulk mail)	An alternate Application Setting can be applied, which has queue management options disabled
Remove access to Large File Send (LFS), which can be used to send large files or directories outbound	High-risk user cannot try to use LFS as a point of data-exfiltration	An alternate Application Setting can be applied, which has LFS options disabled

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.