HENNGE One

Tadrill Utilization Guide

HENNGE Customer Success Division

Note

- The information in this document reflects the service status as of March 2025 and is subject to change without prior notice.

- For users on the HENNGE One Basic plan:
  - The suspicious email reporting feature (Tadrill Alert) is not available.
  - Usage is limited to two times per user per year (January 1 to December 31).

Expected Effects

Expected Effects

Prevention of Malware Infections

Enhancing the Ability to Identify Suspicious Emails

- Expand employees' knowledge to recognize suspicious emails through training exercises of varying difficulty.
- Repeated training not only improves response skills in specific scenarios but also builds daily awareness of the risks associated with suspicious emails.

Prevention of Spreading Malware Infections

Enhancing the Ability to Respond to Suspicious Emails

- Establish consistent procedures for handling suspicious emails.

Employees

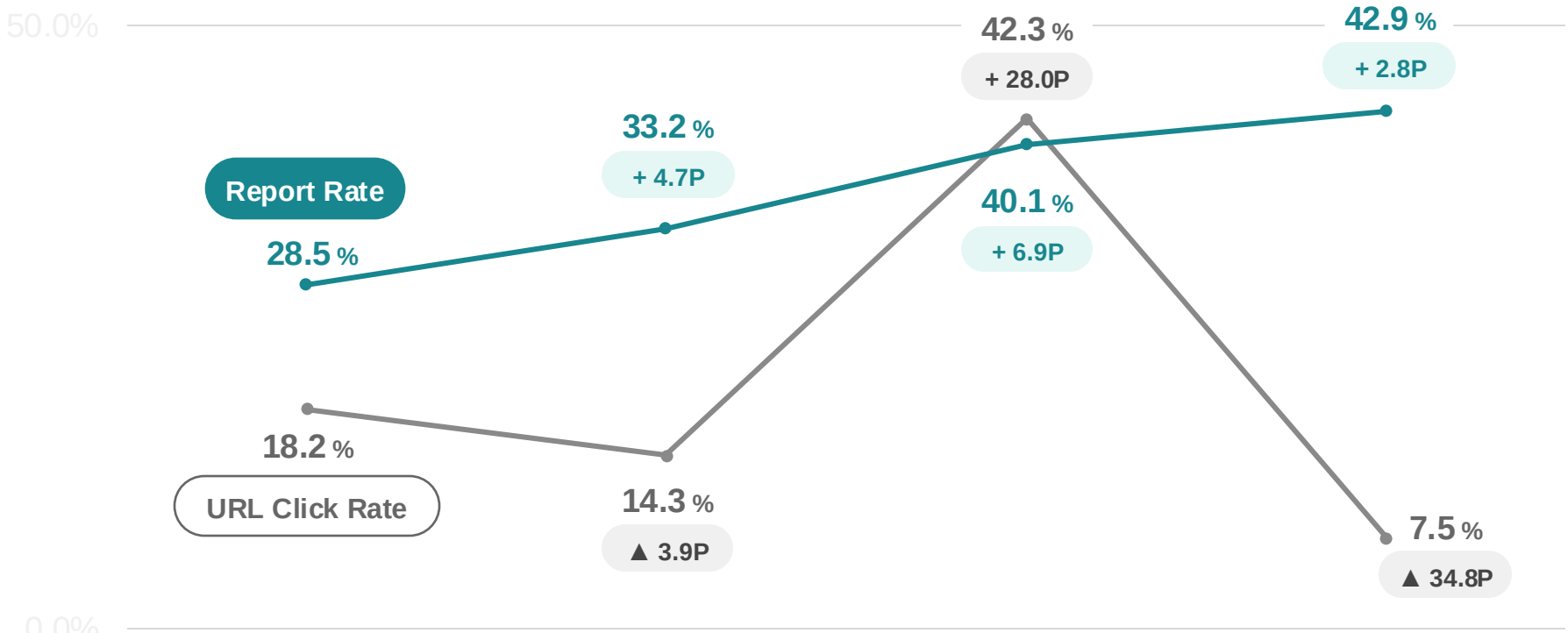
- ✓ Report any suspicious emails immediately.
- ✓ If a URL is clicked or a file is opened by mistake, report the incident without delay.

Administrators

- ✓ Define a process for receiving and responding to reports, and ensure all reports are handled following the process.

Typical Transition of Training Results

Although the URL click rate may vary depending on the email scenario, the reporting rate consistently shows an upward trend with repeated training.



Training Scenario (Example)	1st	2nd	3rd	4th
	Missed call – Includes an attachment labeled as details.	Event invitation – Appears to be from an executive using a spoofed name.	Security system update – Uses the name of an actual employee to announce a new system.	System alert – Notifies about personnel changes, mimicking internal alerts.

Training Flow

Training Flow

1. Design

Plan the training schedule, email content, and objectives.
Develop the overall training strategy.

2. Training

Distribute the training emails to users.

3. Feedback / Review

Analyze training results, including click and report rates.
Evaluate performance against the original objectives.

4. Follow-up

Provide feedback or additional guidance based on user performance.
Plan and prepare for the next training cycle.

Training Design

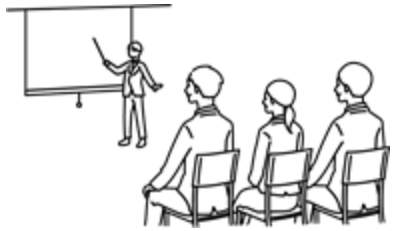
Training Design

Consideration Items	Contents
Timing	When will the training take place? What's the duration?
Objective	Define goals (e.g., raise awareness of the reporting function, confirm security awareness).
Notification Policy	Notify in advance / No notice / Raise awareness of specific attack types only.
Distribution Method	All at once / Randomly / Immediately.
Target Audience	All employees or selected groups (e.g., by department, entry year, position).
Type	Email types: URL link / File download link / Attachment.
Email Content	Adjust difficulty level, theme, and sender identity.
Click/Open Rate (Target)	Set target rates (typical: 10–20% for clicks/opens).
Reporting Rate (Target)	Set target reporting rate (typical: 20–30%).
Post-Training Follow-up	Share results with employees, plan retraining if needed.

Training Design

Consideration Items	Contents
1. Announcement	Decide whether to notify employees in advance about the training.
2. Email contents	• Sender address / Display name • Subject / Message body • Should it be easily identified as a training email?
3. Training period	Determine the duration of the training.
4. Training dispatch	Choose the delivery method: all at once or randomly.

Training Design - 1. Announcement



Consideration Items	Announce in advance	Warn about Phishing Mail	Practical Training
Recommended Usage	First-time training	First-time or subsequent training	Second-time training onward
Merits	Minimizes end-user confusion (e.g., fewer inquiries)	Boosts awareness through education and measures training effectiveness	Simulates real-life conditions and clarifies organizational/user response capability
Demerits	Limits realism; hard to simulate real-world phishing	May confuse users if the training is not clearly recognized	May cause user confusion
How to Convey	- Explain training purpose - Show how to use the system - Share schedule	- Raise awareness of suspicious emails - Explain how to respond and use tools	

Example of Emails to Notify of Reporting Function Using Tadrill

By using Tadrill to conduct a simulated exercise to inform about Tadrill alert (reporting function), it is possible to confirm whether users reported as instructed.

Subject	[Training Email] Please report with Tadrill
Message	To Whom It May Concern @@@This email is a training email@@@ Please report this email according to the procedure by [Month DD (Day of the week) HH:MM]. Please check the following page for reporting procedures: [Manual URL]. Please note that this is a send-only address and we cannot respond to replies. If you have any questions, please contact ○○. Thank you for your cooperation.

Training Design - 2. Email Contents

1 Sender/Display Name

- Use unfamiliar email addresses and display names that users wouldn't normally see from companies, organizations, or individuals they know.

2 Title/Body

- Craft titles that entice users to open the email and consider reporting it.
- Make the body clear and relevant to the simulated scenario (e.g., urgent notices, bonuses).
- Include elements where users are likely to be cautious and embed detection points.

3 Difficulty Level

- Use realistic and sophisticated camouflage that causes hesitation to report.
- Low difficulty: easily spotted but may test reporting behavior.
- High difficulty: may lead to clicks without reporting.
- Adjust difficulty based on the training objective.

Training Design - 3. Training Period

During Tadrill training creation, only link clicks and reporting actions performed within the period set as the [training end date] will be recorded.

Training Design - 4. Training Dispatch

	Send all at once	Send randomly
Merits	• Training can be implemented in a short period.	• Because it arrives at different timings for each user, it is difficult for them to notice it's a training email.
Demerits	• There is a possibility that users sitting near each other, etc., will spoil the content for each other.	• There is a possibility that users who receive the training email early will spoil the content.
Usage Scenarios	• When work locations are scattered. • To quickly grasp the training implementation status. • To inform about the reporting function.	• To minimize the possibility of users noticing it's a training email.

Training Email Verification

Training Email Verification

Prior to deployment, administrators are encouraged to use the test training mode to send verification emails to multiple recipients.

During training email verification, please verify the following:

- Training emails should arrive in the inbox, not the junk/spam folder.
- User-specific tags and links within the training email body function as expected.
- For training emails with links, verify that they direct to the correct pages.
- Link click and attachment open records for training emails are verifiable on the Tadrill management screen.
- Reports related to training emails are verifiable on the Tadrill management screen.

Review / Feedback

Review Points - Ability to Identify Suspicious Emails

Points:
✔ Was the training implemented without a significant gap from the previous training (within 3-5 months)?
✔ Did the link click rate and file open rate clear the target values?
✔ Were detection points set appropriately within the training email?
✔ For users who "clicked", was education provided to raise awareness of the detection points and prevent recurrence?
✔ For users who did not "click", is it understood whether they recognized the detection points?

Review Points - Ability to Respond to Suspicious Emails

Points:
✔ Did the reporting rate clear the target value?
✔ Is the flow for reporting suspicious emails established, and are training emails being reported according to it?
✔ Is the flow after receiving a report of a suspicious email defined?
✔ Is the flow after a user clicks a link or opens a file in a suspicious email defined?
✔ Can guidance be provided to individuals who failed to report after clicking a link or opening a file?
✔ Has the reason and background for why reporting is important been communicated to users?

end