NESIL

# User Guide

*Data Security Awareness and Simulation Platform*

Platform and interface guide · Step by step from campaign creation to reporting

nesil.ai · Version 1.0

# Table of Contents

This guide is designed to teach the platform step by step, from beginner to advanced level. Each section comes with screenshots and numbered instructions; red boxes and numbers point exactly to the places you need to click.

23. Tracking Domains
24. SMTP Configuration
25. Webhooks
26. API Keys
27. Integrations

## ACCOUNT AND SETTINGS

28. Settings
29. Quick Reference and Frequently Asked Questions

# 1. What is Nesil?

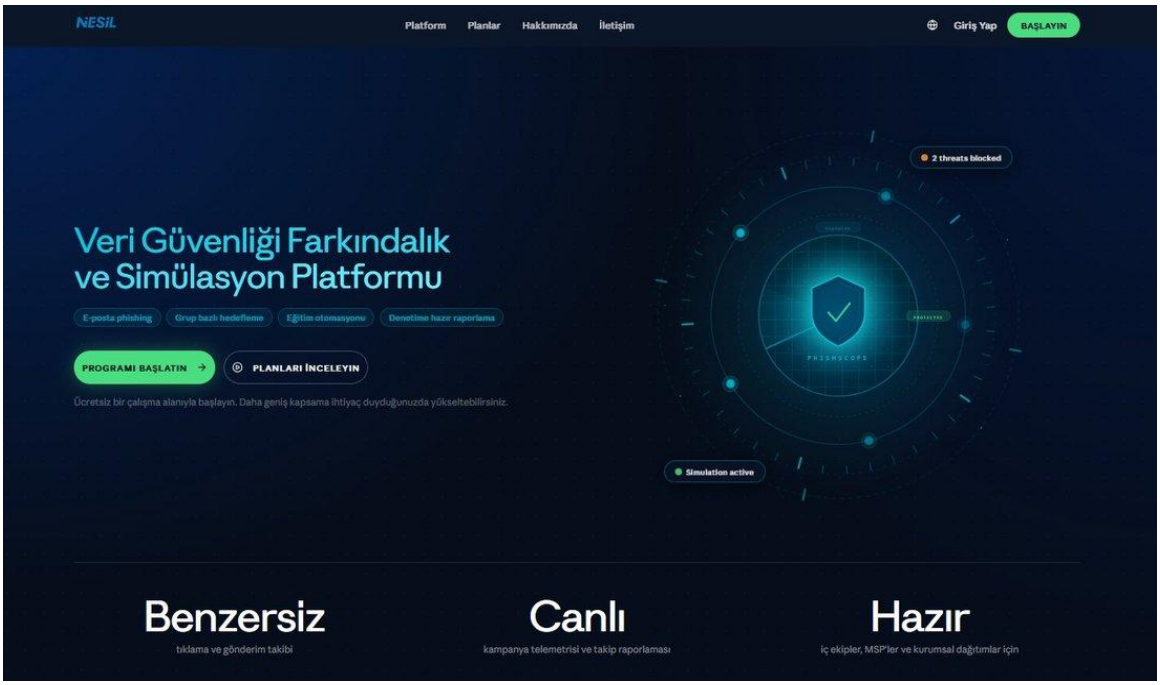
Nesil is a platform that enables organizations to safely simulate phishing attacks targeting their employees, measure the results, and reduce human-caused security risk through awareness training.

The goal is to send emails that closely resemble the techniques used by real attackers, to see which messages employees fall for and which they do not, and to assign tailored training based on this data. The entire process—from campaign planning to target list management, from click tracking to department-level risk scores and SIEM integrations—is managed from a single dashboard.

## Who is it for?

- Information security teams (SOC, CISO office) — for regular phishing drills
- IT administrators — to measure team security maturity
- Compliance teams (ISO 27001, KVKK, GDPR) — to document training records
- MSPs and managed security providers — to run for multiple clients
- HR and training departments — to provide hands-on security training for new hires

## What does the platform do?




*Nesil's public welcome page. Dark theme, cyan-accented typography, and the top menu; the Platform, Plans, About Us, and Contact pages are accessible from here.*

In summary, the platform brings together the following core capabilities:

- Designing phishing campaigns with realistic email templates
- Managing target lists individually, in bulk via CSV, or in groups
- Real-time tracking of every event such as sending, opening, clicking, and form submission
- Generating a unique, personalized tracking link for each target per campaign
- Automatically calculating risk scores at the department and organization level
- Assigning ready-made security awareness training modules to groups
- SMTP, Slack, Teams, Jira, Splunk, PagerDuty, and custom Webhook integrations
- Programmatic access and automation via API keys
- Tracking every operation with KVKK/GDPR-compliant audit logs

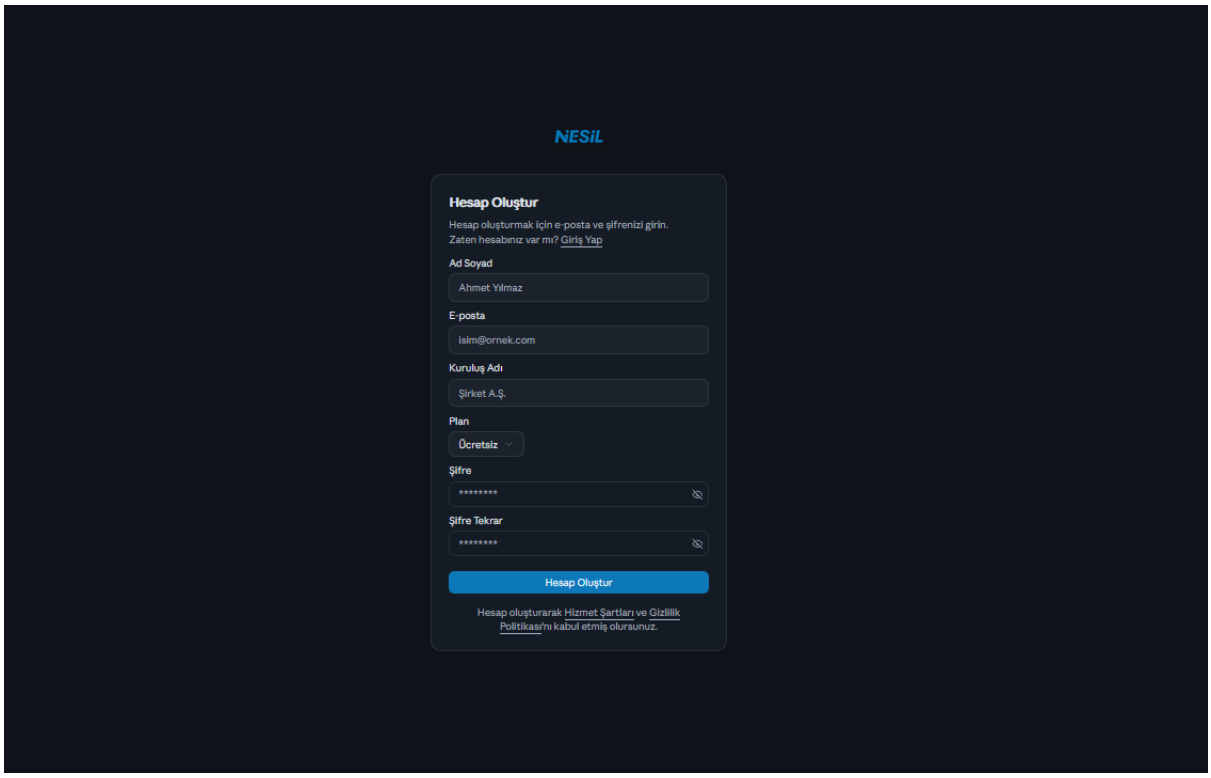
## How to read this guide?

Each section of the guide follows the same structure: first, the relevant screen is introduced as a whole, then the points you need to click are marked on the screenshot with red boxes and numbers. Immediately after, these numbers are explained in order, and step-by-step usage scenarios are provided where needed. At the end of each section, tips and warnings related to that area are collected in separate boxes.

> **If you are using it for the first time**
>
> We recommend reading in order. First try account creation and the interface tour, then try a mini test campaign with the "Creating a Campaign" section.
>
> Then move on to the templates and target groups sections — you can only set up a real scenario once these are ready.

# 2. Account Creation

To use the platform, you first need to create an account. The account represents the secure workspace where all of your organization's campaigns, templates, target lists, and reports are stored.




*The Create Account screen. Fields are listed from top to bottom and all are required (except Plan).*

## Field-by-field descriptions

1 **Ad Soyad** Your real name as it will appear on the platform. You can change it later from the Settings > Profile menu.

2 **E-posta** The primary email linked to your account. Password resets, important notifications, and system alerts are sent to this address. Using a corporate address is recommended.

3 **Organization Name** The display name of your company or team. For example, "Nesil Technology." This name appears in reports, audit logs, and team invitations.

4 **Plan** Choose your starting plan from options such as Free, Starter, Pro, or Enterprise. You can upgrade as your needs grow.

5 **Password** Set a strong password. It must be at least 8 characters and include uppercase letters, lowercase letters, numbers, and special characters.

6 **Confirm Password** Re-enter your password exactly to prevent typos.

7 **Create Account** If all fields are correct, click the button to create your account. A moment later you will be automatically redirected to the dashboard.

**Not sure which plan to choose?**

The free plan is sufficient to get to know the platform and run a small test campaign. If you plan to set up a real organization-wide simulation, starting with the Enterprise plan will let you proceed without hitting limits.

The plan can always be changed later from the "Settings > Organization" menu.

**Choose your organization name carefully**

The organization name appears in emails sent to team members you invite and in audit logs. While it can be changed later, doing so may cause inconsistencies if invitations have already been sent to many users.

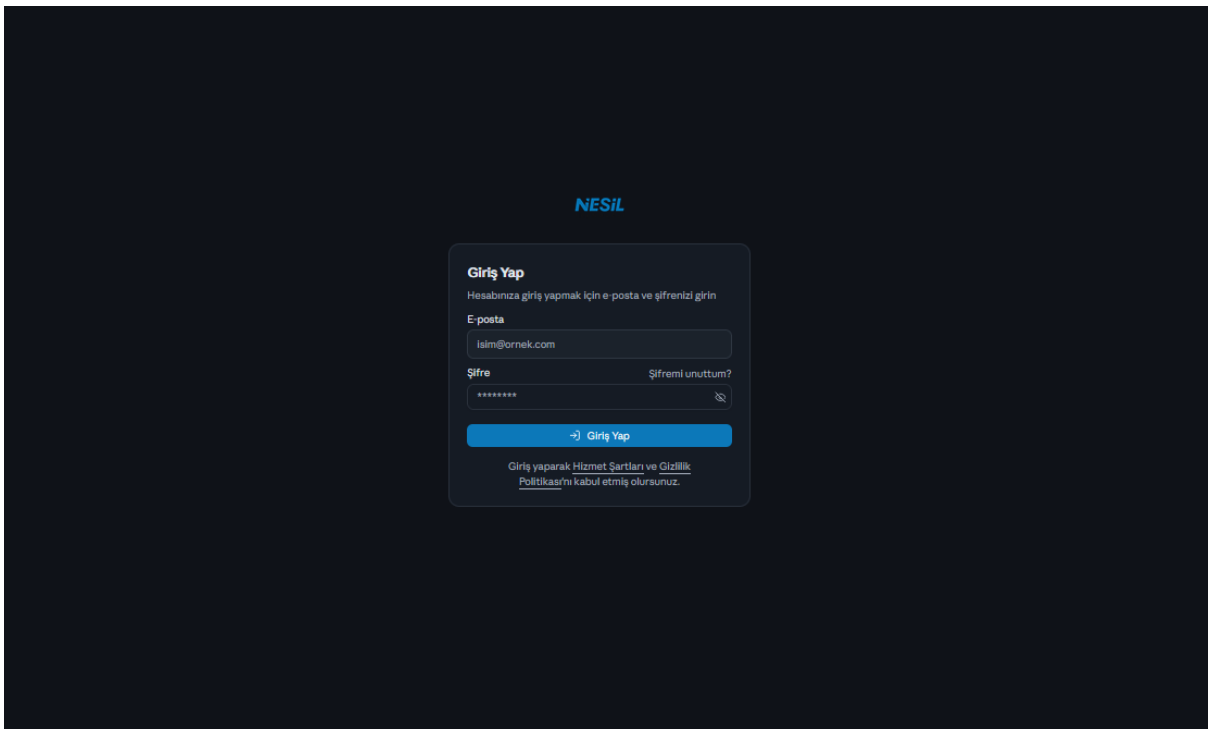
## After creating your account

The system directs you straight to the dashboard. Recommended steps after the first login are:

- Go to the Settings page via the gear icon in the top right and complete your profile and organization information.
- Configure your own sending server in the "SMTP" settings (required for real campaigns).
- Browse the ready-made gallery in "Email Templates" and select a template to adapt for your organization.
- Invite the administrators you will need from the "Team" menu.

# 3. Log In

After creating your account, you use the Log In screen each time you access the dashboard. The screen is simple and focused on one purpose: letting you in securely.




## Field-by-field descriptions

1 **E-posta** Enter the address you used when creating the account. The field is not case-sensitive.

2 **Password** Type your password. You can click the eye icon on the right to make it visible and verify what you typed.

3 **Forgot my password** If you cannot remember your password, click here. A secure reset link will be sent to your email address.

4 **Log In** If all information is correct, press the button and go directly to the Dashboard.

**Session duration**

By default, the session remains open for a certain period of time. If you are working on a shared device, remember to use the "Log Out" option from the profile menu in the top right when you are done.

## Forgot my password flow

A simple three-step flow is followed to reset your password:

1. **E-posta girin** When you click the "Forgot my password" link, enter your account email in the form that appears.

2. **Gelen kutunuzu kontrol edin** Nesil sends you a reset link. The link expires shortly for security purposes.

3. **Set a new password** Click the link and create a new strong password of at least 8 characters.

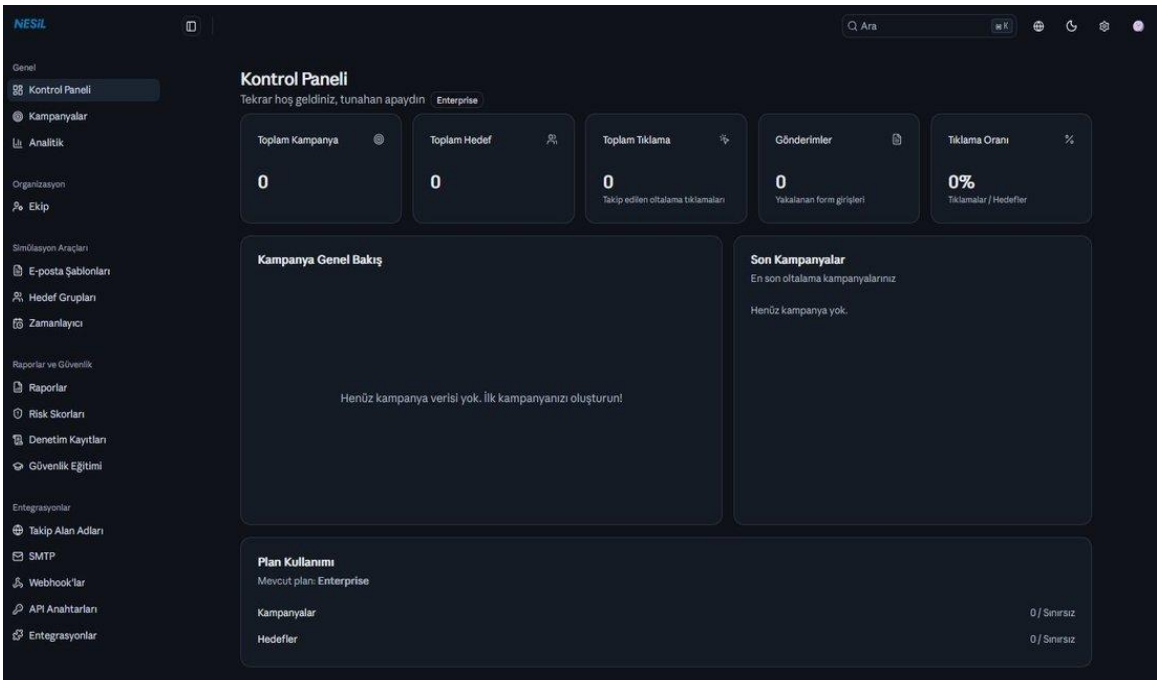
**E-posta gelmediyse**

First check your spam folder. Wait a few minutes and try again if it does not arrive.

If it still does not arrive, make sure the address you entered is the one you used when creating the account. Some organizations may block emails from certain domains due to corporate filters — in this case, contact your IT team.

# 4. Interface Tour

Nesil's admin panel consists of three main areas: the navigation menu on the left, the toolbar at the top, and the workspace in the center. In this section we examine what each area is for — so that in the following sections you can find it immediately when a particular screen is mentioned.




*Full view of an empty dashboard with no campaigns created yet.*

## Main areas

1 **Left navigation menu** All the main sections of the platform are accessible from here. The menu is divided into five main headings according to functional groups: General, Organization, Simulation Tools, Reports and Security, Integrations.

2 **Top KPI cards** Shows a summary of the most critical metrics such as total campaigns, targets, clicks, submissions, and click rate at a glance. These cards update live as campaigns run.

3 **Campaign Overview** A line chart showing the performance of your active and past campaigns over time. Ideal for trend analysis.

4 **Recent Campaigns** A summary list of the campaigns you most recently ran. For each one, the click count and status badge are visible; clicking a row takes you directly to that campaign's detail page.

5 **Plan Usage** Shows how close you are to the limits of your current plan. If you are on an unlimited plan, only usage counters are shown here.

6 **Profile and quick access** The language selector, theme switcher (light/dark), settings, and your profile avatar are located in the top right.

## Structure of the left menu

The left menu offers a total of sixteen functional modules under five main groups:

### Genel

- Dashboard — General summary and recent activities
- Campaigns — List of all your simulation campaigns
- Analytics — Performance comparison across campaigns

### Organizasyon

- Team — Management of users with access to the platform

### Simulation Tools

- Email Templates — Ready-made and custom phishing emails
- Target Groups — Department-based organization of target lists
- Scheduler — Automatic launching of campaigns

### Reports and Security

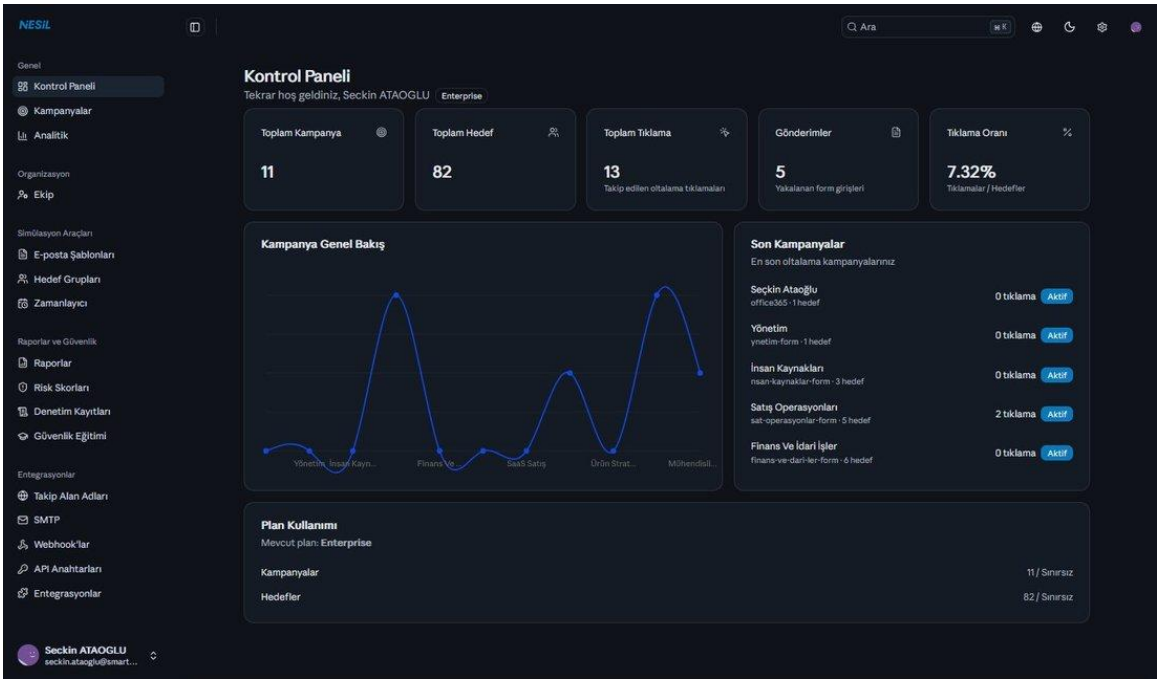
- Reports — Detailed campaign and department reports
- Risk Scores — Organization-wide risk assessment
- Audit Logs — Immutable log of all administrative operations
- Security Training — Awareness training modules and assignments

### Integrations

- Tracking Domains — Custom domain for branded campaign links

- SMTP — Email sending server configuration
- Webhooks — Real-time event notifications to third-party systems
- API Keys — Credentials for programmatic access
- Integrations — Slack, Teams, Jira, Splunk, PagerDuty, and custom targets

## This is how the dashboard looks when a campaign is running



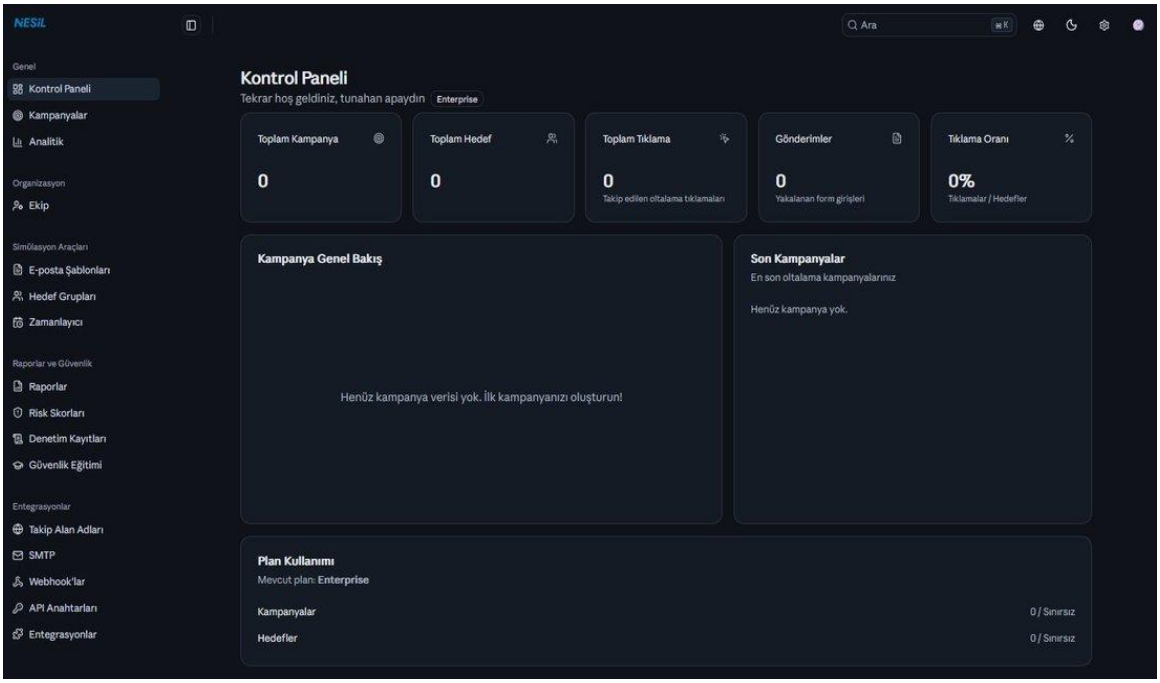

*Live dashboard view of an organization with 11 campaigns, 82 targets, and 13 clicks. The chart is enriched with real data; the "Recent Campaigns" list shows a status badge on each row (Active/Draft/Completed).*

> **Tip for working efficiently**
>
> Identify the three or four menus you will use most frequently (e.g., Campaigns, Analytics, Email Templates). Your daily workflow likely revolves around these. Other menus are only visited when setting something up (e.g., SMTP) or at reporting time (Audit Logs).

> **Keyboard shortcuts**
>
> You can instantly focus the search box in the top right with ⌘K (Mac) or Ctrl+K (Windows) on your keyboard. As the platform grows and the number of modules increases, this shortcut saves time.

# 5. Dashboard

The Dashboard is the first screen that greets you every time you log in to the platform. Its purpose is simple: to show you at a glance where to start your day. Here, instead of waiting for answers to questions like "how many campaigns do I have," "has the click rate gone up since last week," "am I approaching the plan limit," you simply see them.




*Empty Dashboard view with no campaigns created yet. All KPIs are zero and the chart is empty; the system encourages you to create your first campaign.*

## Top KPI cards

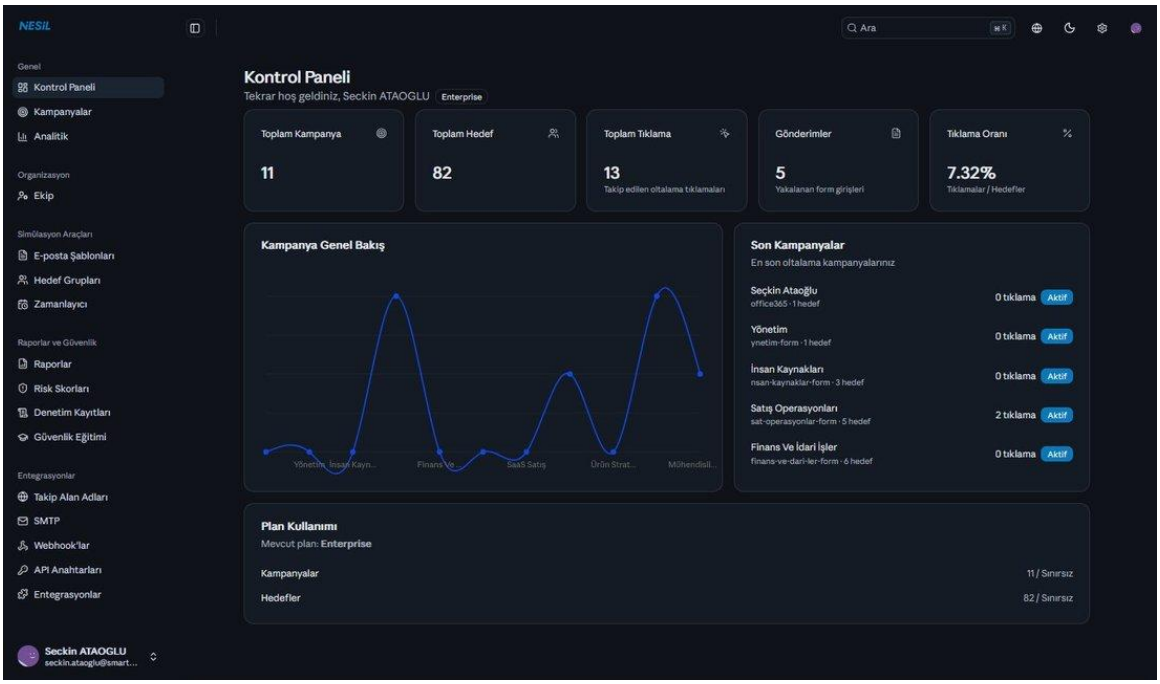
The five cards at the top of the dashboard summarize the overall state of your organization's security awareness:

- Total Campaigns — The number of all campaigns created so far (including drafts, active, and completed).
- Total Targets — The number of unique targets added to campaigns.
- Total Clicks — Total clicks made on tracked phishing links.
- Submissions — The number of targets who entered credentials into target forms (i.e., the number of targets who "took the bait").
- Click Rate — Ratio of total clicks to total targets. As this value decreases, it means organizational awareness is increasing.

> **What do these metrics tell us?**
>
> The "Submissions" count is always less than or equal to the "Clicks" count — because a user may click the link but still not submit the form. The difference gives the percentage of users who were "aware but stopped when alerted"; this is a very valuable metric.
>
> Aim to repeat training until your click rate drops below 5%. A 5-10% range is normal even for the best organizations in the world.

## Campaign Overview chart

This area shows the performance of your campaigns as a time series. The horizontal axis progresses by campaign, the vertical axis by metric value. You easily spot trends in this chart: if the click rate drops as the number of campaigns increases, it means awareness is growing.




*A populated Dashboard: 11 campaigns, 82 targets, and 13 clicks. The chart marks each campaign's performance as a dot and connects them with a line.*

## Recent Campaigns section

This list in the top right corner of the dashboard shows the five most recently created campaigns as a summary. Each row contains the campaign name, the template code below it (e.g., office365), target count, total clicks, and a status badge (Active / Draft / Inactive). You can click any row to go directly to that campaign's detail page.

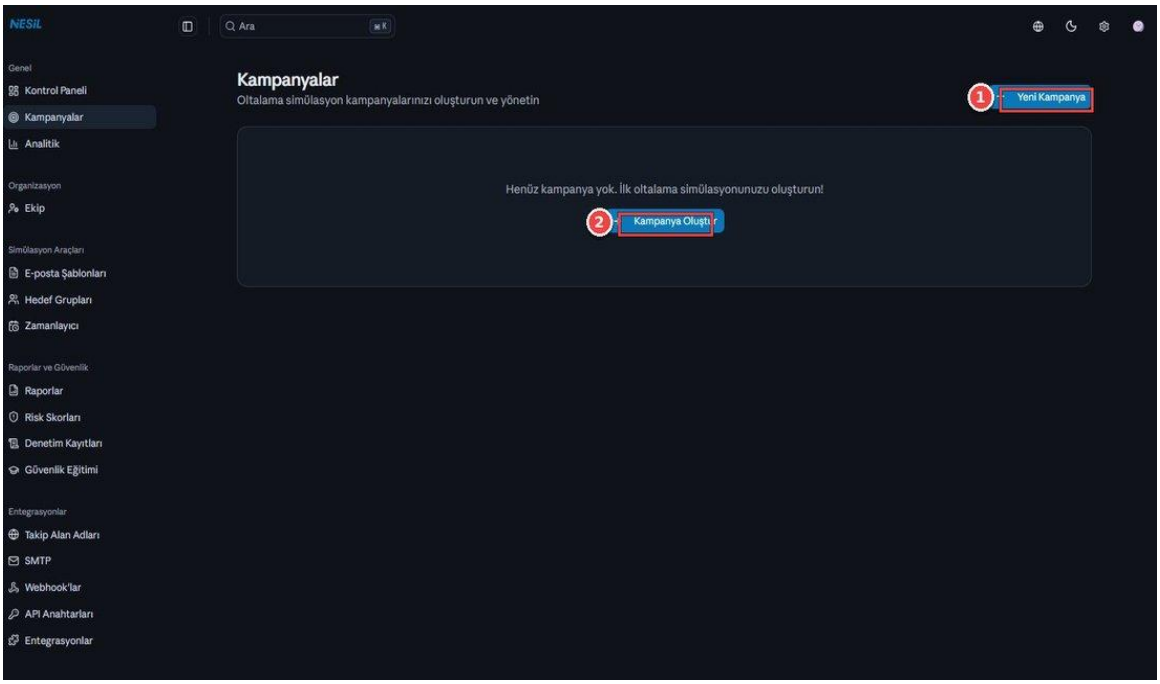
## Plan Usage

The Plan Usage section at the very bottom shows how close you are to the limits of your current plan. If you are on the Enterprise plan, the "Unlimited" label appears; on more restricted plans, percentage progress bars appear.

> **When you approach the plan limit**
>
> If your campaign or target limit exceeds 80%, the dashboard shows you a warning. In this case, you can either upgrade your plan from the Settings > Organization section, or free up space by archiving old, completed campaigns.

# 6. Campaigns

The Campaigns menu is the heart of the platform. Each phishing simulation is defined here as a "campaign" and managed individually. If no campaigns exist yet, the system directs you to create your first campaign.



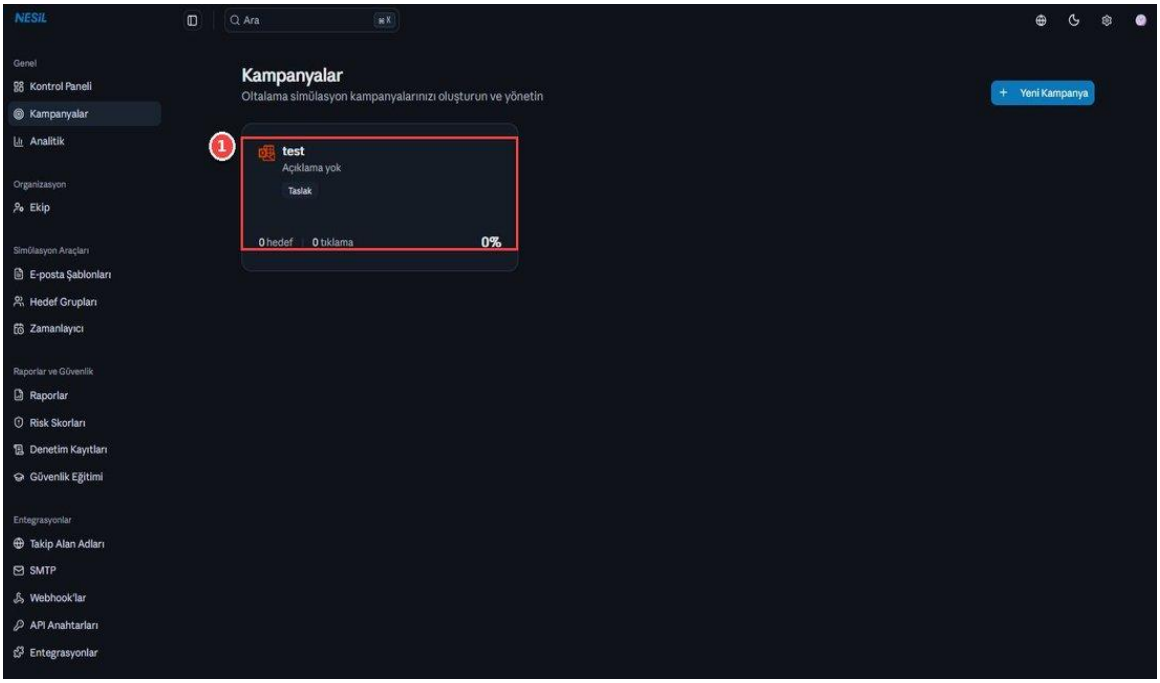

*Empty Campaigns screen. The "Create Campaign" button in the center and the "New Campaign" button in the top right do the same thing — you can start by clicking either one.*

## Ekrandaki kontroller

**1** **+ New Campaign (top right)** The primary button always visible in the top right of the screen. Use this to start a new simulation.

**2** **+ Create Campaign (center)** The central button visible only when no campaigns exist yet. Opens the same modal.

## After creation: list view




*The Campaigns screen after your first campaign is created. The campaign card shows the name, description, status badge (Draft, Active, Completed), target count, total clicks, and click rate all together.*

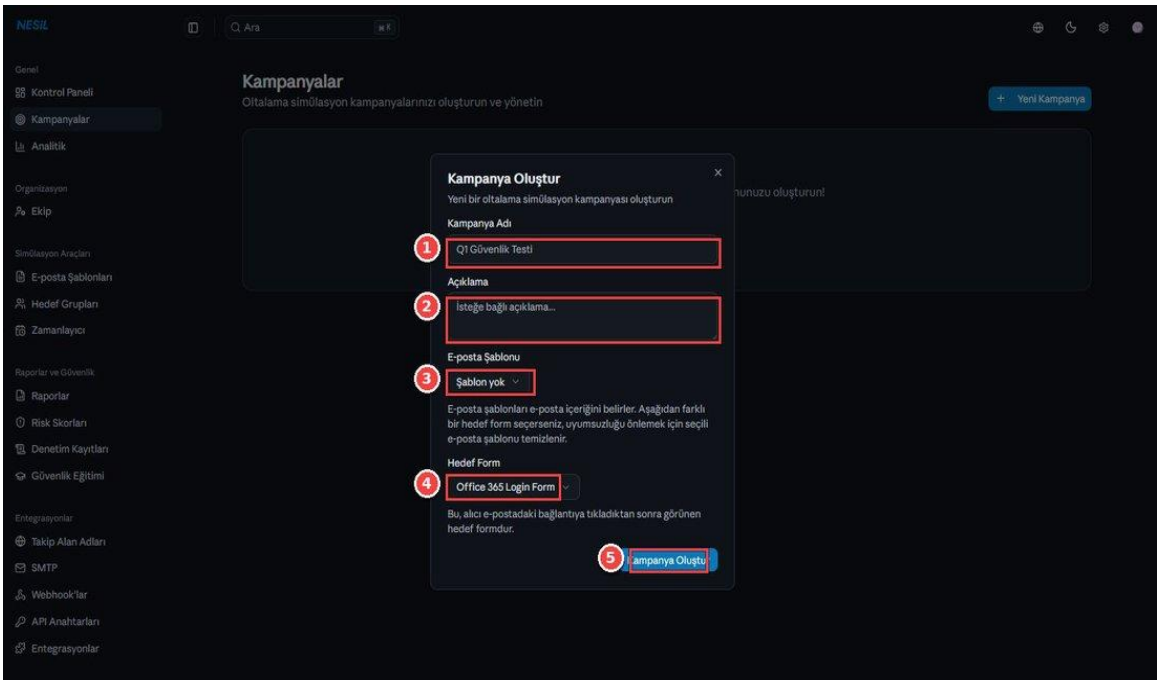
Each card carries summary information and takes you to its own detail page with a single click:

- Campaign name in the top left and its description below (or "No description" if empty)
- Status badge: Draft (not yet launched), Active (submissions ongoing), Inactive (stopped), Completed
- Target count, click count, and click rate in the bottom row
- Large percentage in the top right corner — so the click rate is visible at a glance

> **Read the status badges correctly**
>
> Draft: Created but the "Launch Campaign" button has not been pressed yet. No submissions are made in this state.
>
> Active: The submission flow has started, links are clickable.
>
> Inactive: Manually stopped; can be restarted.
>
> Completed: Reached the planned end date or all submissions to targets are complete.

# 7. Creating a Campaign

Creating a new campaign is one of the most critical operations on the platform. The modal looks simple, but each field has a strategic role. In this section we will explain why each field is important and how it should be filled in real scenarios.




## Field-by-field descriptions

**1** **Campaign Name** The name that distinguishes this campaign from others. Clear, short names containing a date are recommended. Example: "Q1 Security Test", "February 2026 - Finance Department".

**2** **Description (optional)** A free-text field where you can note the purpose, target audience, and expected outcome of this campaign. Very useful when sharing reports with your team.

**3** **Email Template** The template for the phishing email to be sent to targets. You can start with "No template" and change it later, or select one of the ready-made templates from here.

4 **Target Form** The fake form that will open after the user clicks the phishing link. This should match the story told by the email template (e.g., Office 365 alert → Office 365 login form).

5 **Create Campaign** When all fields are filled, press the button. The campaign is saved as a "Draft" and you are automatically redirected to the detail page.

## Template and form compatibility

The note in the center of the modal is very important: "If you select a different target form below, the selected email template will be cleared to prevent incompatibility." What does this mean? The system automatically tries to maintain template + form consistency.

Examples:

- "Office 365 Password Reset" template → "Office 365 Login Form" target form (consistent)
- "Dropbox Shared File" template → "Dropbox" target form (consistent)
- "Google Security Alert" → "Office 365" form? Inconsistent — the user will be suspicious and will not fill out the form.

**Naming tips**

Include the department, quarter, and scenario together in campaign names: "HR - Q1 2026 - Fake Resume Attached".

This discipline will save you a lot of time when preparing reports six months later.

Do not leave the description field empty. Even a short note like "Sales team tested with Dropbox scenario" will be critical later.

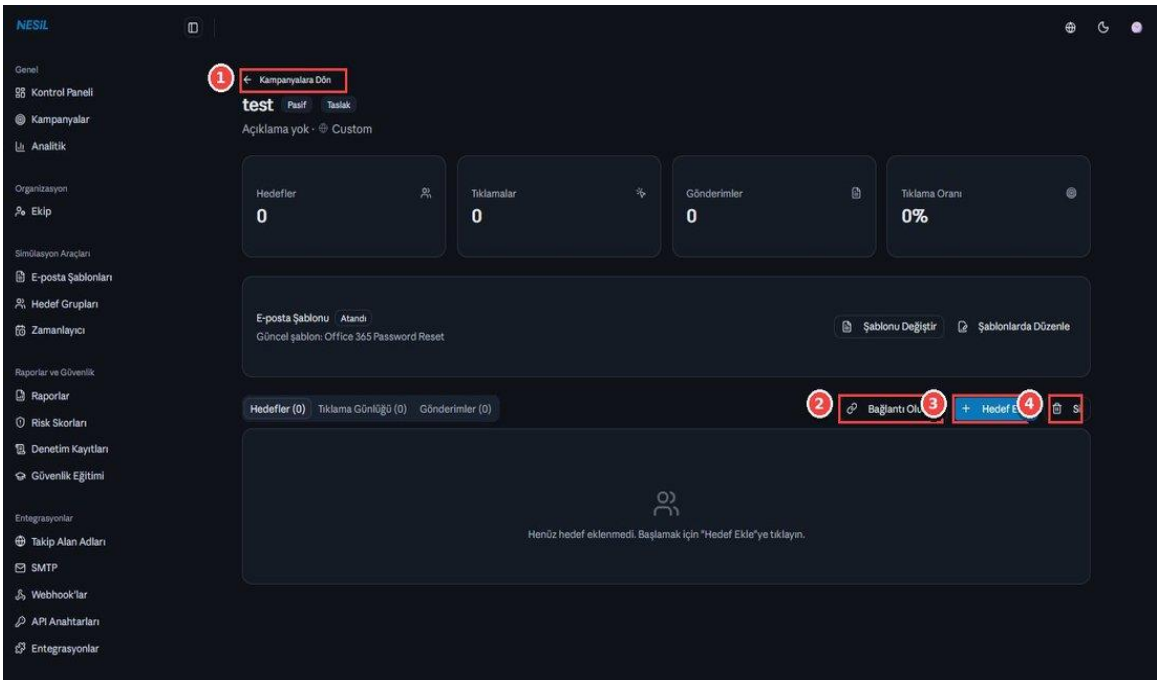
**Verify two things before launching**

The subject and sender address of the email template must be able to pass through your corporate security filters.

If the target form URL is to be generated via a configured tracking domain (e.g., mail-security.yourcompany.com), complete the "Tracking Domains" settings first.

# 8. Campaign Detail and Launch

When a campaign is created, you are automatically redirected to the detail page. This page is designed for you to manage the entire lifecycle of the campaign: adding targets, generating links, launching, monitoring, and deleting.




*Detail page of a newly created campaign with no targets yet. Status: Inactive and Draft. Email template is assigned but submission has not yet started.*

## Areas on the page

**1** **Back to Campaigns** The link in the top left. Always visible and takes you back to the list screen.

**2** **KPI strip** Targets, Clicks, Submissions, and Click Rate — four critical metrics. Updated live as the campaign runs.

**3** **Email Template** The name of the assigned template is shown. With the two buttons on the right, you can change the template or edit it directly in the template gallery.

4 **Three tabs** Targets, Click Log, and Submissions. These tabs show three different perspectives of campaign data.

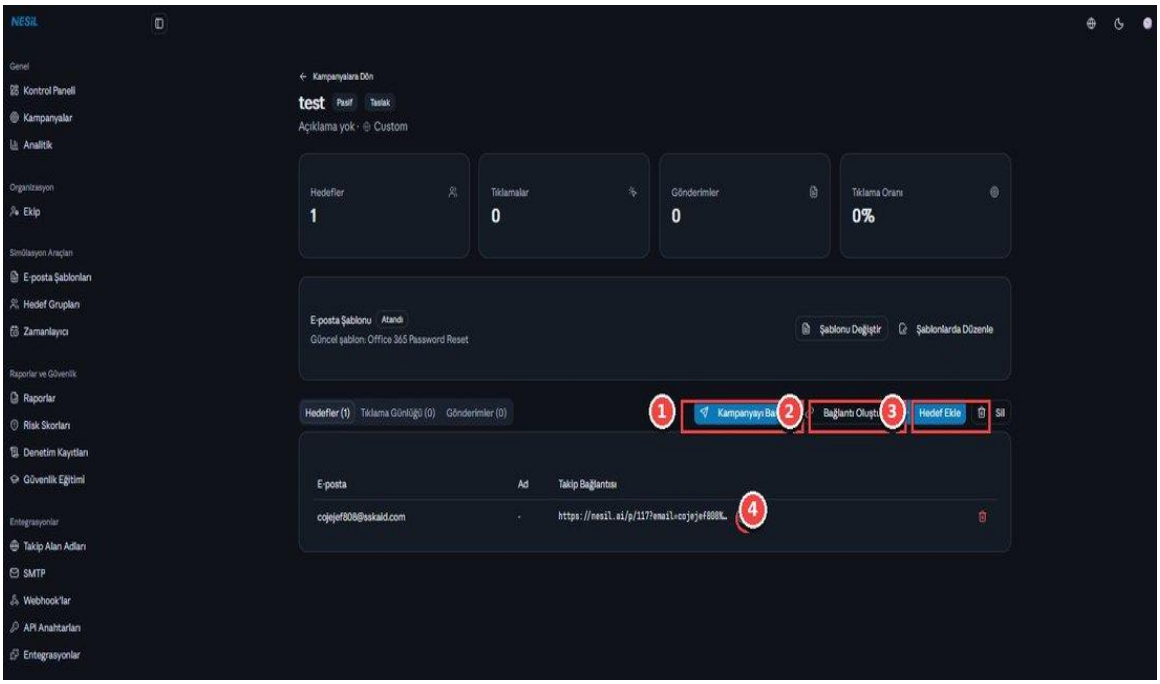
5 **Generate Link** Generates a personalized tracking link for a single target. Useful for manual tests.

6 **Add Target** Adds new targets to the campaign. Options include individual, bulk, or importing ready-made groups.

7 **Sil** Permanently deletes the campaign. Cannot be undone — use with caution.

## Launching the Campaign

After creating a campaign and adding at least one target, only one step remains to start sending: pressing the "Launch Campaign" button. This button appears on the right side of the tab strip when there are one or more targets in the campaign.




*Campaign detail page after one target has been added. The "Launch Campaign" button (1) has become active, and the target's email address and the generated tracking link are visible in the row.*

1 **Launch Campaign** The moment you press the button, the system starts sending your email template to every target in the campaign. The status changes to "Active" and tracking timers start running.

2 **Generate Link** Generates a custom tracking link for a manual test target.

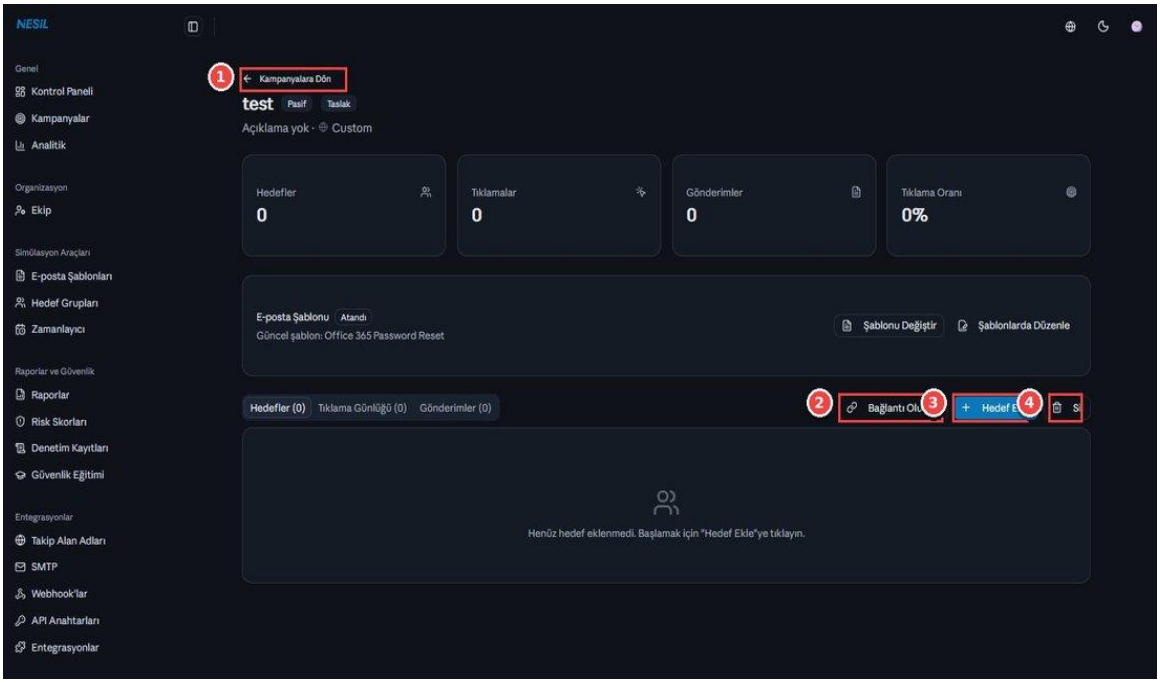
3 **Add Target** You can add targets to a running campaign later too; new targets will receive separate submissions.

4 **Copy tracking link** The copy icon on the right side of the row; allows you to easily get the link for manual testing.

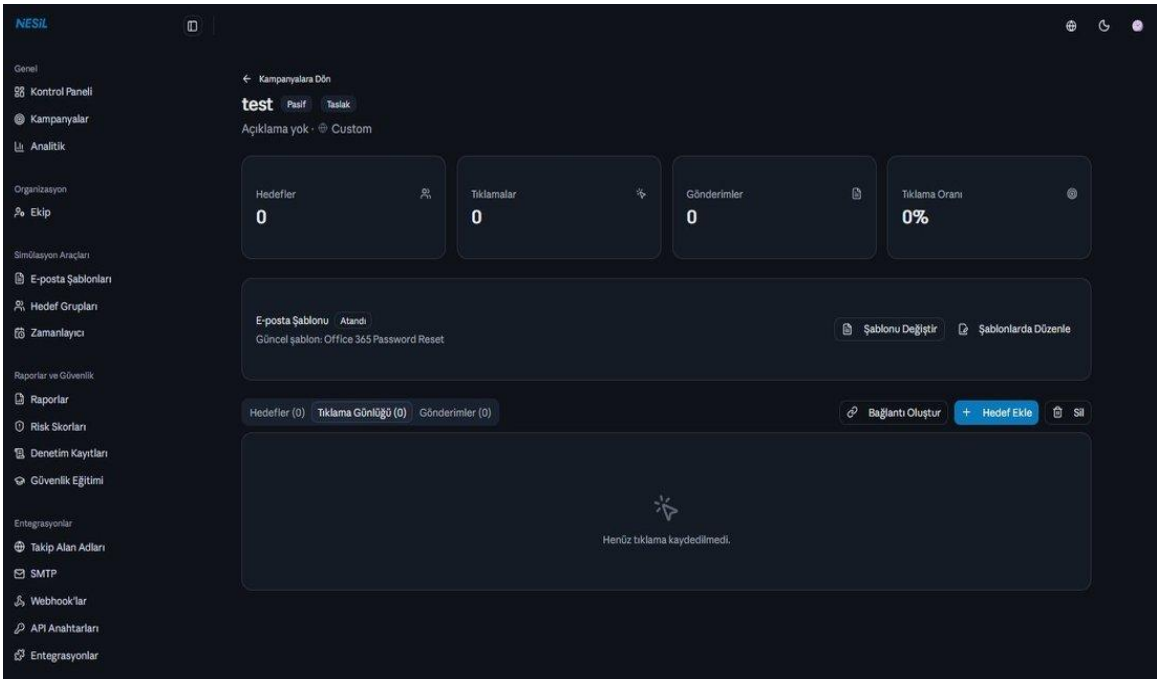
5 **Delete row** Removes a single target from the campaign. The overall campaign statistics are preserved but no further submissions are sent to that target.

> **Pre-launch checklist**
>
> 1) Has at least one target been added? 2) Has an email template been assigned (visible on the Campaign Detail page)? 3) Has SMTP configuration been completed? 4) Has the tracking domain been configured? If all these steps are complete, the campaign will start smoothly.
>
> If SMTP is not configured, the system will warn you and will not start sending — first complete the configuration from the Integrations > SMTP menu.

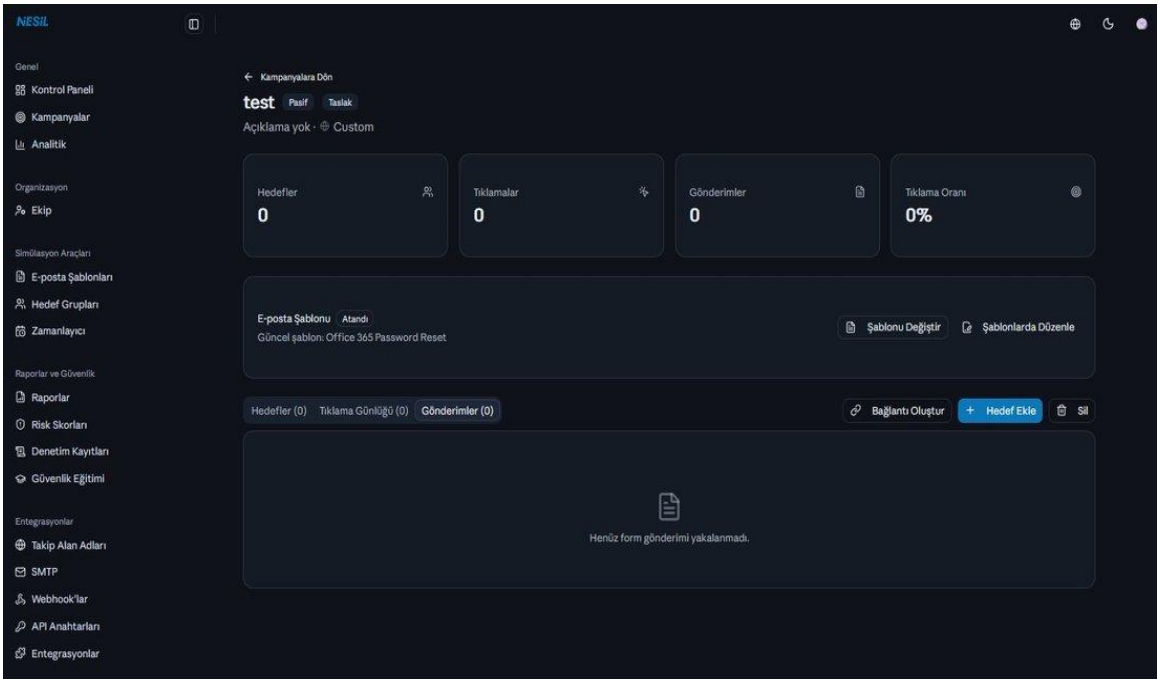
## Three monitoring tabs




*Targets tab. An information screen appears when no targets have been added.*




*Click Log tab. Every click event is recorded with a timestamp, IP address, and browser information. Appears empty if there are no clicks yet.*



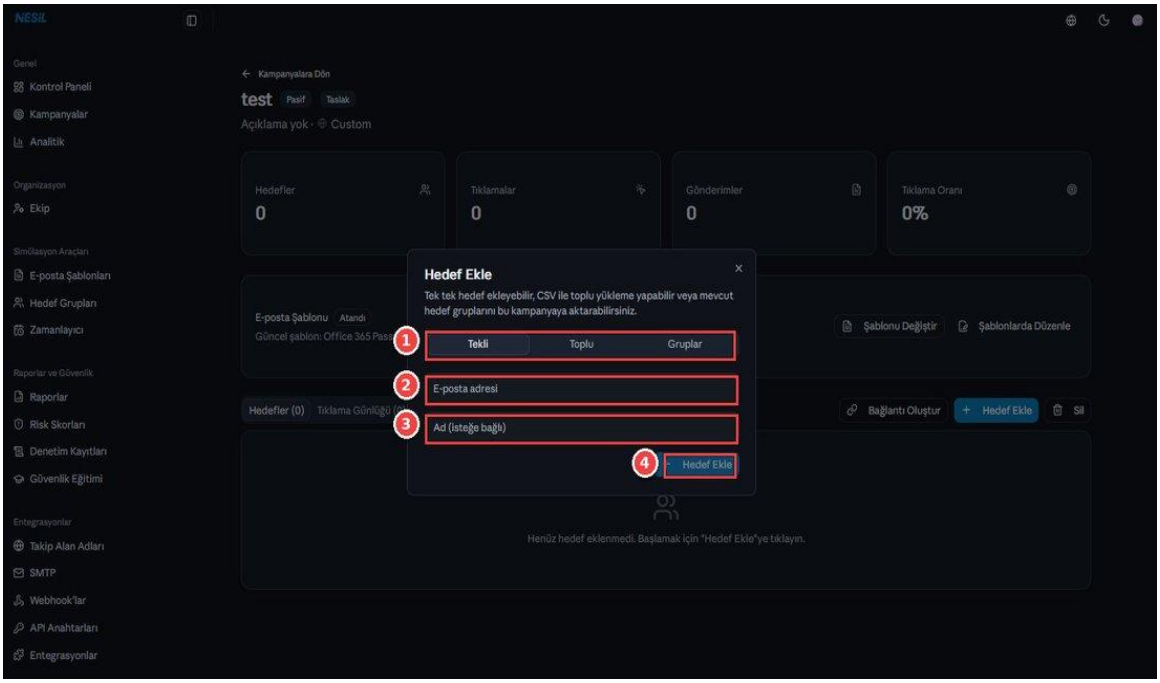

*Submissions tab. Lists the users who submitted credentials to the target form — i.e., those who "took the bait." This is the most important risk indicator.*

> **Reading order for the three tabs**
>
> The numbers in parentheses on the tabs: (0), (1), (5) — show the total number of records in that tab. Look at the parentheses to understand campaign performance at a glance.
>
> The number in the Submissions parenthesis means "how many people provided credentials"; urgent training assignment for these people is recommended.

# 9. Adding Targets

Your campaign is ready and your template is selected; now it's time to determine who to send it to. Nesil offers you three methods: adding one by one manually, bulk pasting, and importing a pre-created target group.

## Method 1: Adding individual targets




*Individual tab — ideal for a quick test or adding a single missing target.*

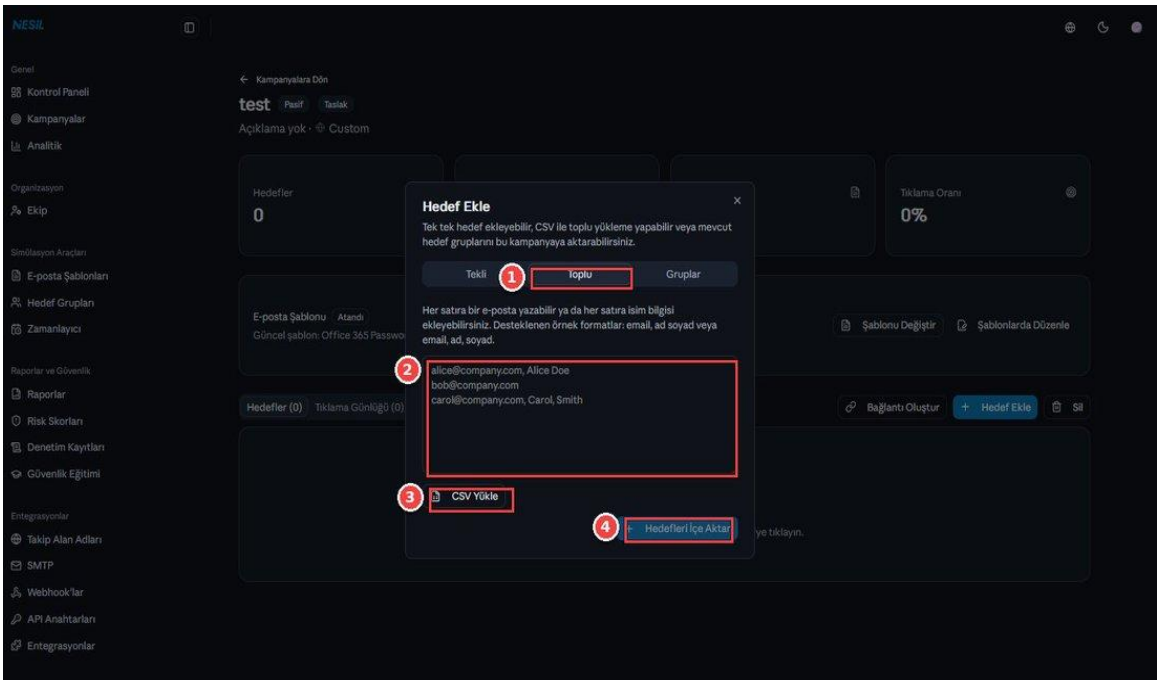
**1** **Tab strip** Switch between Individual / Bulk / Groups. "Individual" is currently active.

**2** **E-posta adresi** Required field. Must be in a valid email format.

**3** **Name (optional)** Used for sending personalized emails. If entered, this name appears in the {{name}} variable in templates.

**4** **Add Target** The target is added to the list and the modal stays open — you can add several targets one after another.

## Method 2: Bulk pasting




*Bulk tab — used to import large Excel lists in a few seconds.*

**1** **Select the Bulk tab** Switch to the "Bulk" tab from the tab strip.

**2** **Paste the list** Write one target per line. Supported formats: email only; email and name; email, first name, last name. Examples are shown in the description below the text box.

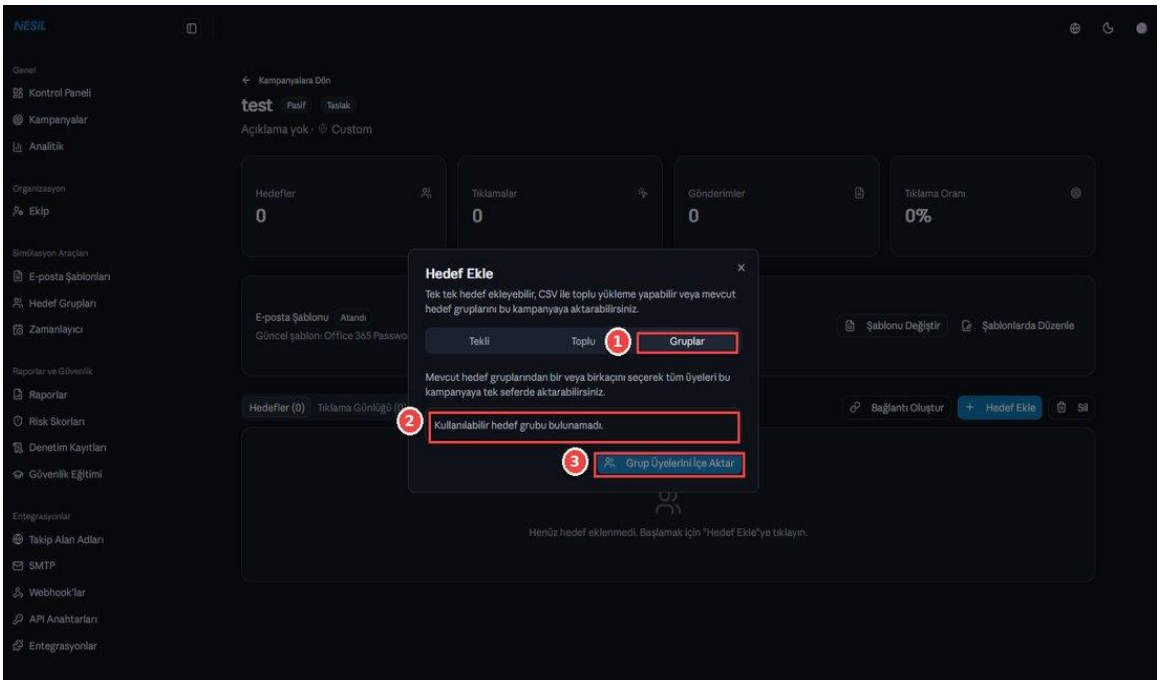
**3** **Upload CSV** If you have a very long list, you can upload the Excel or CSV file directly. The system automatically recognizes headers (email, name, surname).

**4** **Import Targets** All rows are added to the campaign at once. Invalid formats are rejected with a warning.

> **What should the CSV file look like?**
>
> The first row must be a header: email, name (or first_name), surname (or last_name).
>
> Separate columns with commas, and ensure there are no spaces at the beginning or end of email addresses.

> Save in UTF-8 encoding — important to prevent character corruption.

## Method 3: Importing from ready-made groups




*Groups tab. Performs bulk import from lists previously defined in the "Target Groups" menu. Indispensable for department-based campaigns.*

**1** **Select the Groups tab** Switch to "Groups" from the tab strip.

**2** **Select a group** All previously created groups appear in the dropdown. Multiple can be selected.

**3** **Import Group Members** All members of the selected group(s) are added to the campaign at once. If the same email appears in more than one group, the system automatically deduplicates.

> **If there are no previously saved groups**

> The text "No target groups available" appears in this tab. You first need to go to "Target Groups" from the left menu and create a group. We will explain this process in full detail in the following sections.

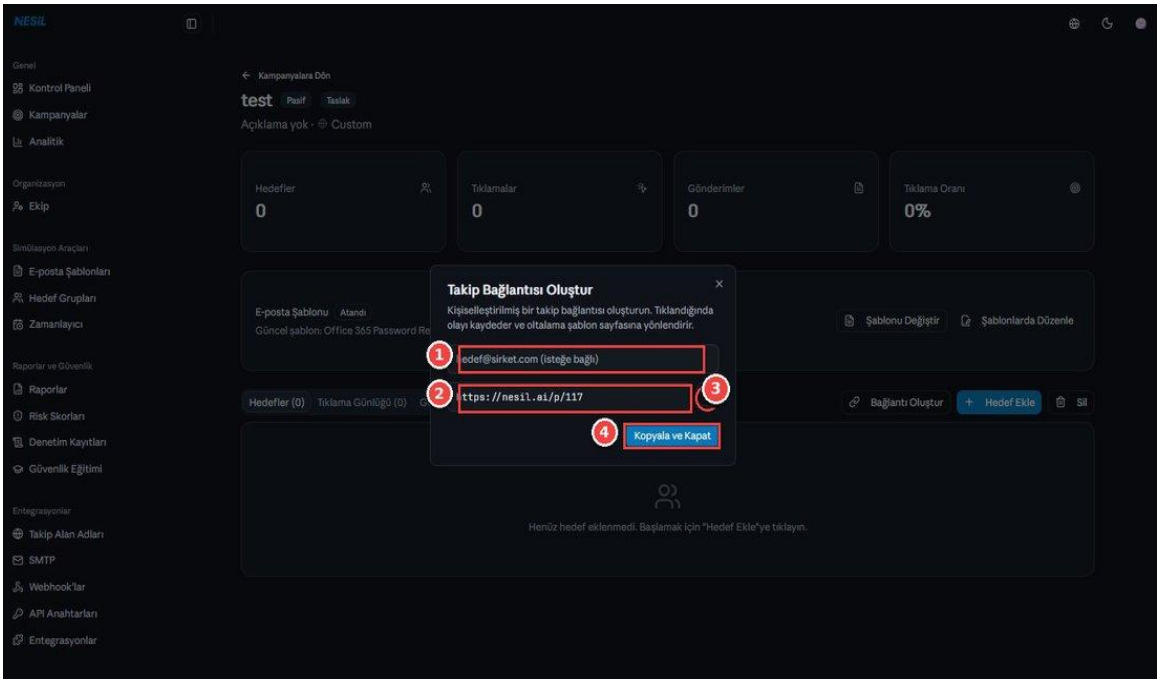
## Which method to use when?

- Individual: For a quick test or to add a single target you missed from the list.
- Bulk: If you have a ready Excel list and are not going to create a group specific to the campaign.
- Groups: If you will use the same list in multiple campaigns — e.g., if the "Sales department" list will be reused in four separate campaigns.

# 10. Tracking Links

A separate "tracking link" is generated for each target. This link is the phishing link inside the campaign email; when clicked, the system records who clicked, when, and from which IP, and redirects the target to the fake form page.

The system creates links automatically, but sometimes you need to do this manually — for example for a test target, or when you want to give it to a specific person by hand. That is when the "Generate Link" button comes into play.




## Field-by-field descriptions

| | |
|---|---|
| 1 | **Target email (optional)** You specify who you are giving this link to. If entered, who clicked appears as a name in the log. |
| 2 | **URL** The tracking link generated by the system. Example: https://nesil.ai/p/117 — p/ is the platform's short path, and 117 is the internal number of the campaign. |
| 3 | **Kopyala ikonu** Click the icon on the right to copy the link to the clipboard. |
| 4 | **Copy and Close** Copies the link and closes the modal with a single touch. |

### How do tracking links work?

Each link is unique. Even if you send the same email to two different targets, each receives a different unique link. This way you can distinguish "Did Ali click, or Ayse?"

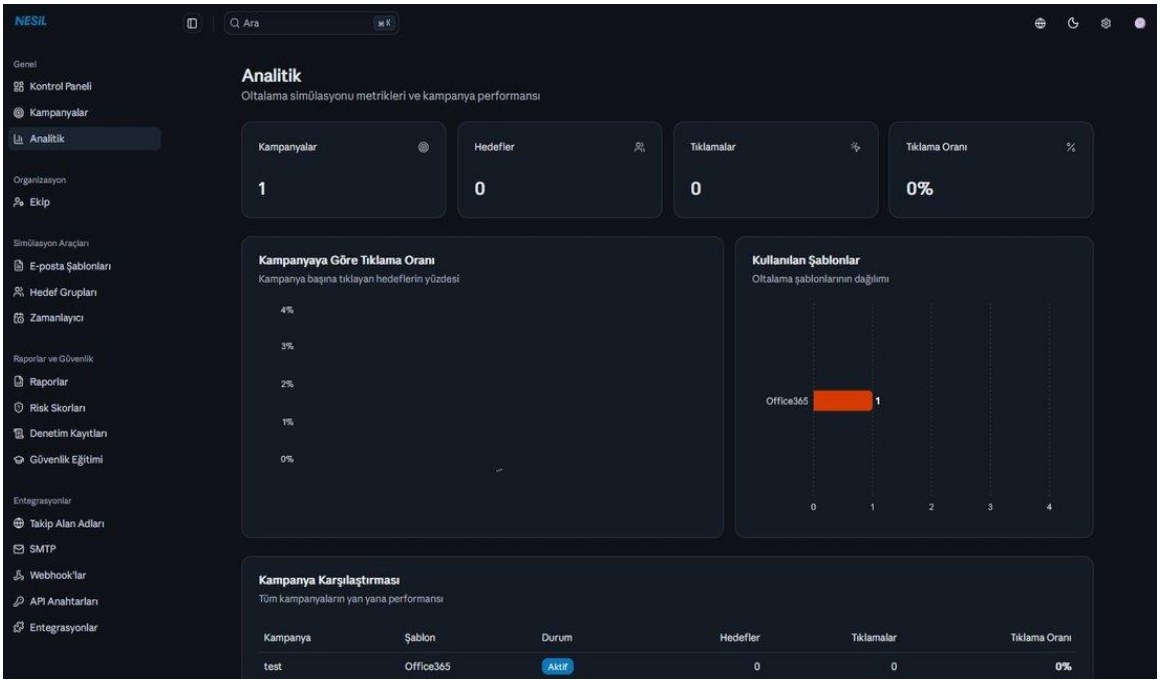
The link usually has a parameter like ?email=... at the end. This parameter is used to identify the person who clicked — do not try to edit it manually, the link will break.

### For branded links

By default, links come in the "nesil.ai/p/..." format. If you want your own branded address (e.g., "security.yourcompany.com/p/...") to be used instead, you need to configure your own DNS record from the "Tracking Domains" page in the left menu. This is explained in detail in section 23 of this guide.

# 11. Analytics

The Dashboard gives you the answer to "what is my current status." The Analytics menu offers a deeper look: answers to strategic questions such as "which scenario was more effective among my campaigns?", "how has my click rate changed over time?", "which template attracted the most interest?" are found here.




## The four main areas of the screen

1

**KPI strip** Total Campaigns, Targets, Clicks, and Click Rate. Same as on the dashboard but filtered here only for the selected campaigns.

2

**Click Rate by Campaign** Shows the click rate of each campaign as a bar or line. You immediately notice the most striking campaign.

3

**Templates Used** A horizontal bar chart showing how many campaigns each template was used in. E.g., the "Office365" template was used in 1 campaign — the chart shows this with a single bar.

4

**Campaign Comparison table** A detailed table presenting all your campaigns side by side. Campaign name, template, status, target count, clicks, and click rate are all visible in a single row.

## Campaign Comparison table

The table includes the following columns:

- Campaign — Its name; clicking on it goes to that campaign's detail.
- Template — The code of the email template used.
- Status — Active / Inactive / Draft / Completed.
- Targets — Total number of targets.
- Clicks — Total number of clicks.
- Click Rate — The division of the two numbers. You can click the column header to sort.

### Using analytics in team meetings

This screen is the foundation of corporate awareness reports. Taking a screenshot every quarter and presenting to management is the easiest way to demonstrate with data that organizational security maturity is improving.

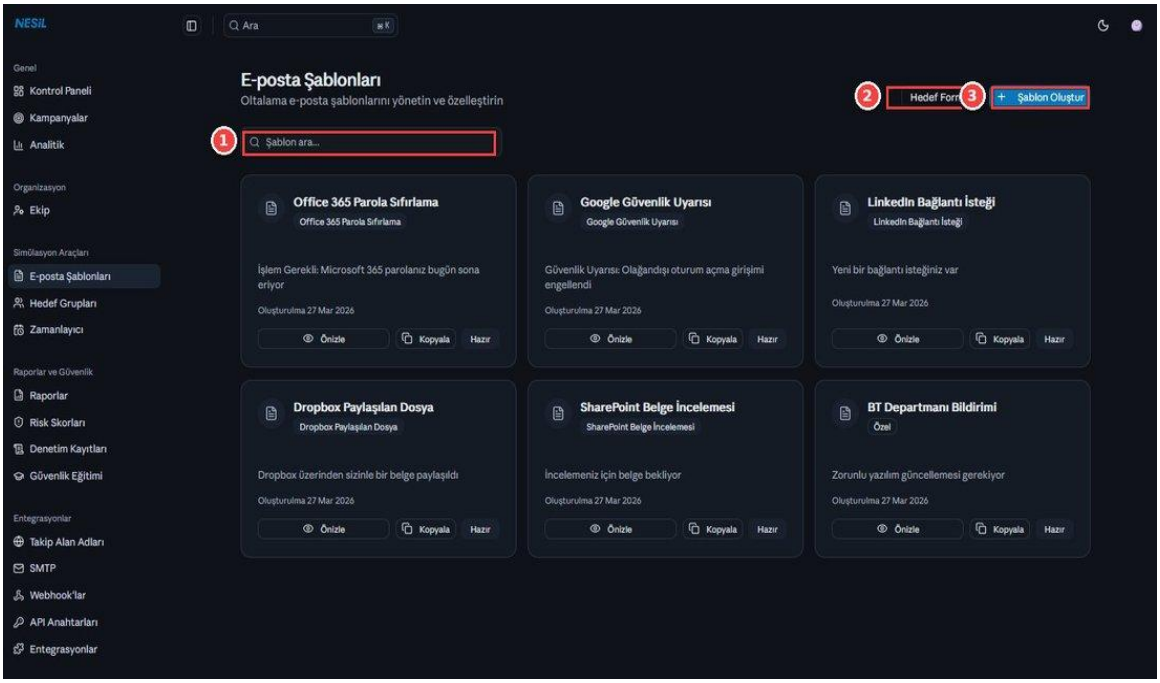
If the click rate dropped from 15% to 4% in 6 months, this is the clearest proof that your strategy is working.

### If there are no campaigns, the chart remains empty

The Analytics screen populates when there is at least one campaign and at least one target. It is normal to appear empty or partially filled in the first weeks of a new organization — the chart becomes meaningful after a few campaigns are run.

# 12. Email Templates

Email Templates are the "voice" and "face" of your campaigns. A good template should be convincing enough to be indistinguishable from a real phishing attack, while still remaining within legal and ethical boundaries. Nesil offers both ready-made gallery templates and allows you to create custom templates from scratch.




*Email Templates screen. Various scenarios (Office 365, Google, LinkedIn, Dropbox, SharePoint, IT department notification) in the ready-made gallery are ready to use with a single click.*

## Ekrandaki kontroller

**1** **Search templates** Searches template names. Becomes indispensable as the list grows.

**2** **Target Forms** Opens the management screen for fake forms (login pages). You can edit ready-made forms or create new ones.

**3** **Create Template** Opens the modal to create a custom email template from scratch.

**4** **Preview** Shows the email + target form preview of the template in a separate modal — ideal for checking before using in a campaign.

5

**Kopyala** Clones the existing template and puts you into editing mode on a copy of it. The safest way to customize ready-made templates without breaking them.

## Anatomy of template cards

In each template card:

- Top row: the template's name (title) and the category code below it (office365, google, linkedin, etc.)
- Middle: the email subject or a short description
- Bottom: creation date and "Ready" badge
- Very bottom: Preview / Copy / Ready action buttons

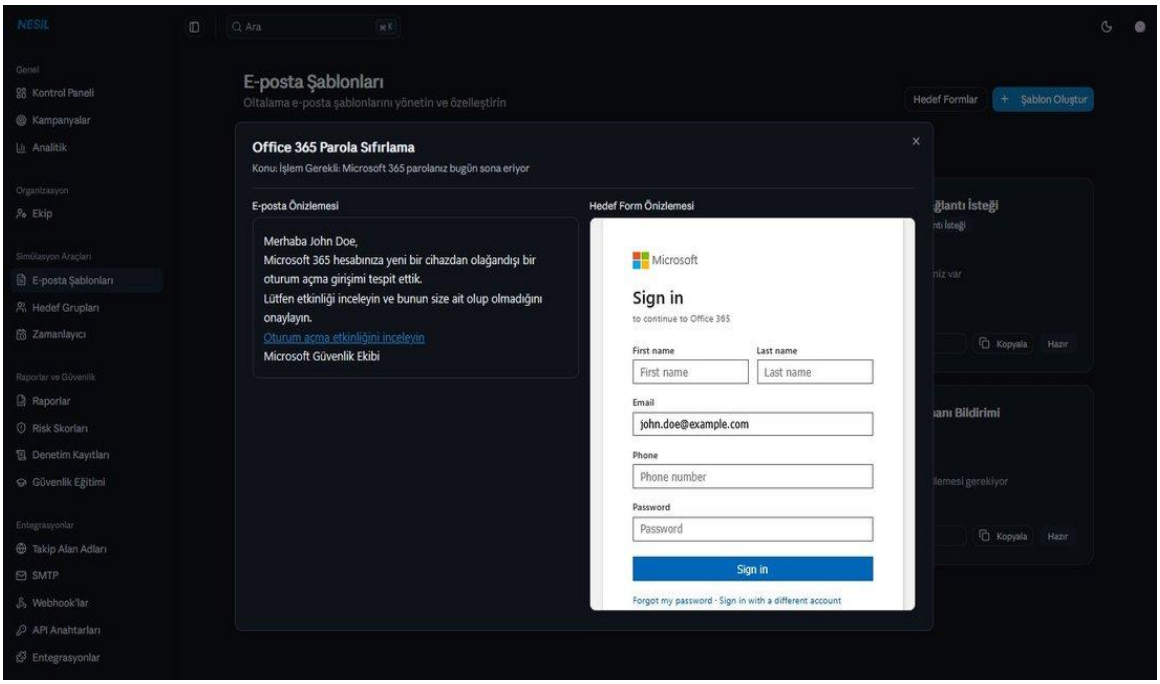
> **Why start from ready-made templates?**
>
> Ready-made templates are inspired by the most common phishing attacks worldwide. Looking at the scenarios in this gallery before starting a campaign both provides inspiration and saves time.
>
> Even if you are going to write your own scenario, duplicating a ready-made template with "Copy" and making changes on it is the safest approach — the HTML structure and variables (e.g., {{tracking_link}}) come correctly set up.

# 13. Ready-Made Template Gallery

Nesil provides the most common phishing scenarios as free ready-made templates. Each template is designed so that both the email text and the target form come together. In this section we will examine each template separately.

## 13.1 Office 365 Password Reset

A classic scenario that comes with a subject line like "Your Microsoft 365 password expires today," directing the user to fill out a form resembling the Office 365 login page. It is one of the most common phishing scenarios in Turkey and worldwide.

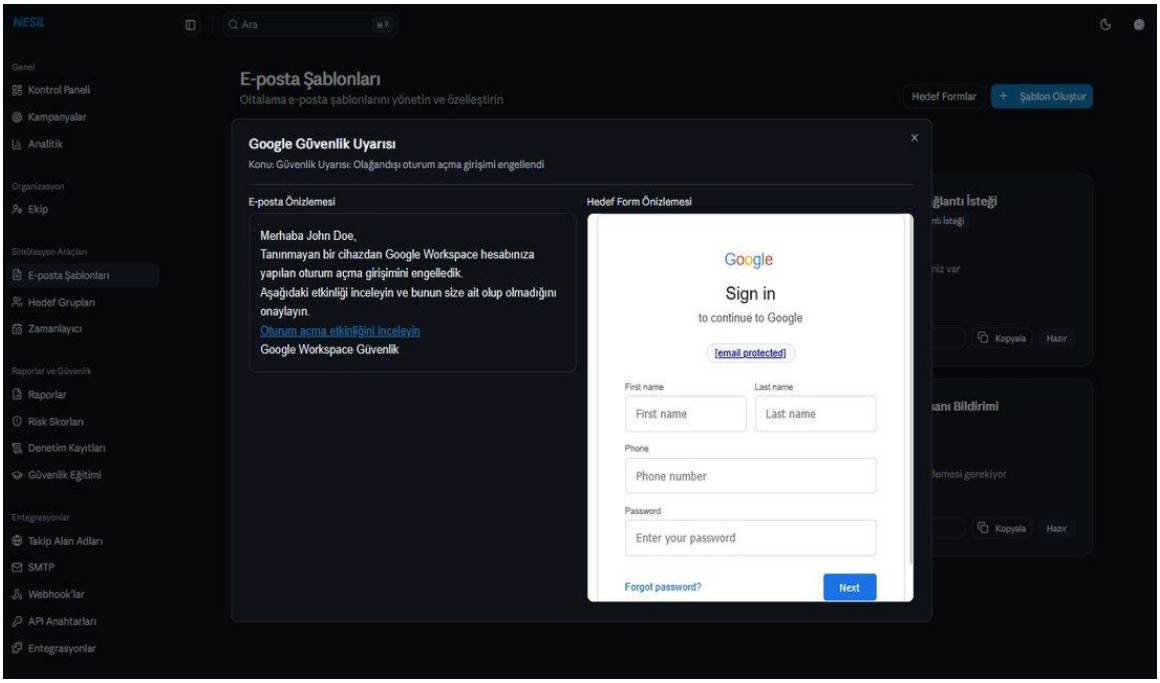



*Left: email preview. Right: target form — almost identical to Microsoft's real login screen. Users can enter information without suspicion because they see this form so often.*

- Who it is for: Almost everyone. Especially ideal as the first test in organizations using Microsoft 365.
- Variables: {{name}} (the person's name), {{tracking_link}} (unique tracking link).
- Expected click rate: Generally 15-25% in the first drill.

## 13.2 Google Security Alert

A scenario that comes with the subject "Unusual sign-in attempt blocked," encouraging the user to immediately intervene in their Google account. Ideal for organizations using Google Workspace.

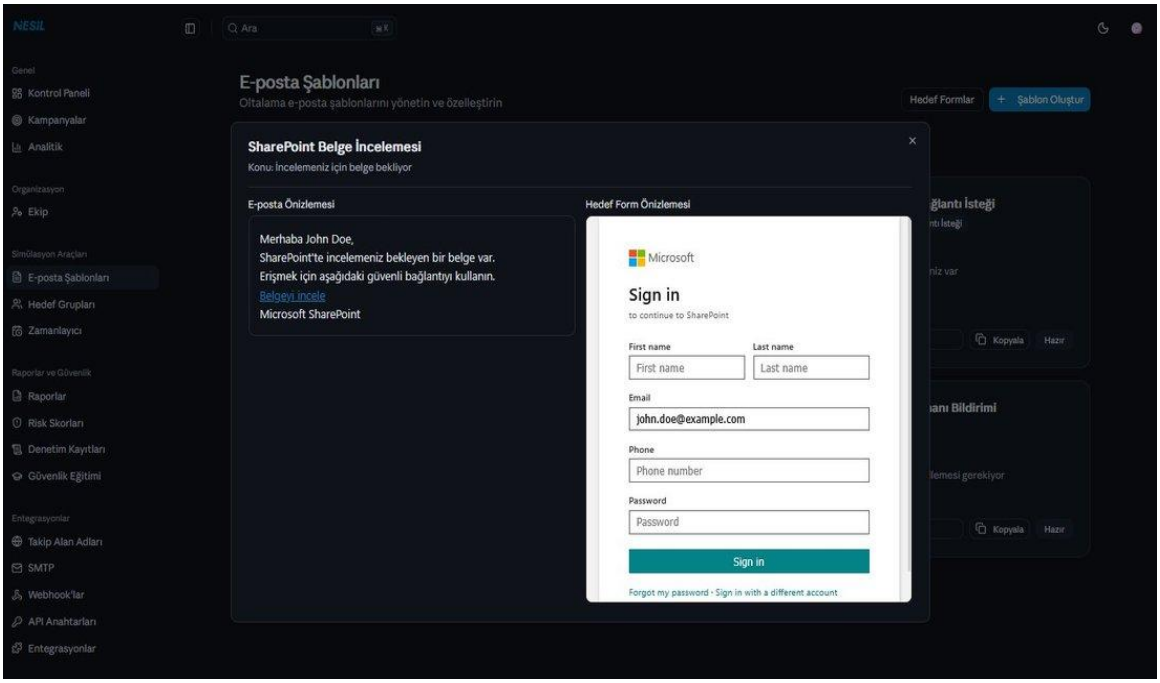



*The email closely resembles the language of Google's real security alerts: "We blocked a sign-in attempt to your Google Workspace account from an unrecognized device."*

- Who it is for: Organizations using Google Workspace (G Suite).
- Note: Google's real alerts look very distinctive; this template is a relatively challenging scenario — the click rate is generally lower than Office 365 (~10-15%).

## 13.3 SharePoint Document Review

"A document is waiting for your review" — a scenario that lures the user with a notification that looks natural within a workflow. It is one of the most effective in corporate environments.

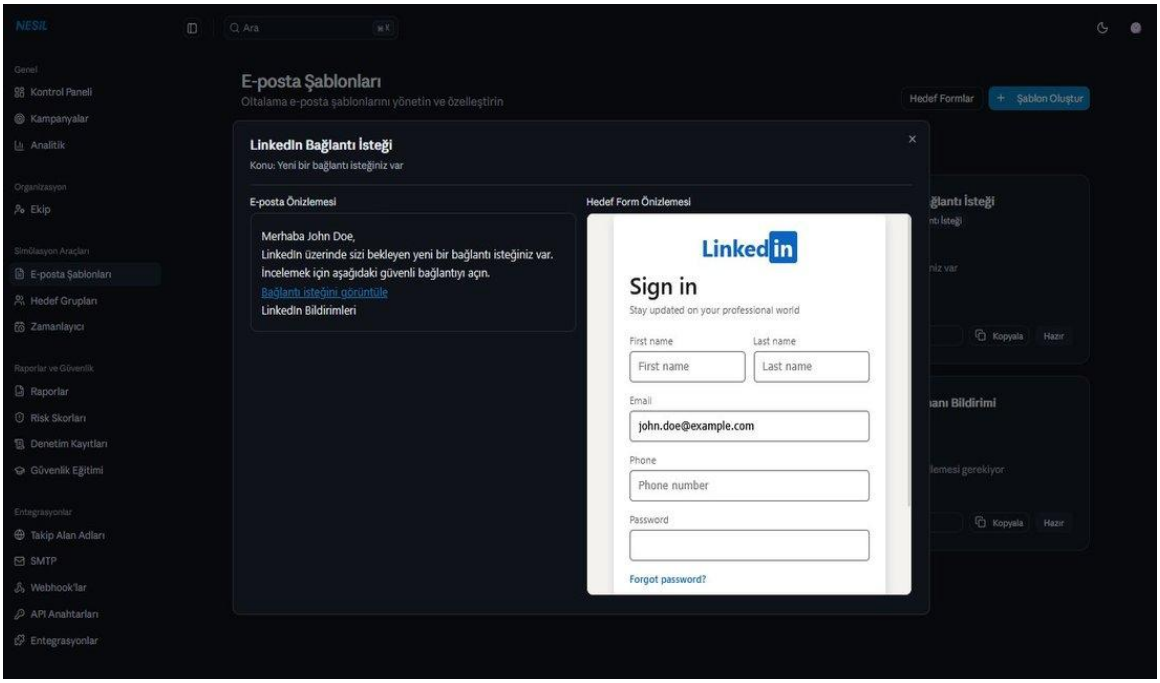



*The form mimics Microsoft's real SharePoint login experience. The user logs in "to see the document" — and has submitted their information.*

- Who it is for: All organizations using SharePoint / OneDrive. Especially departments that frequently share work documents.
- Effective segment: Legal, HR, finance teams — because they review a real document almost every day.

## 13.4 LinkedIn Connection Request

A scenario that comes with "You have a new connection request," triggering professional curiosity. The user clicks the link thinking "who is that?" and lands on a form resembling the LinkedIn login screen.

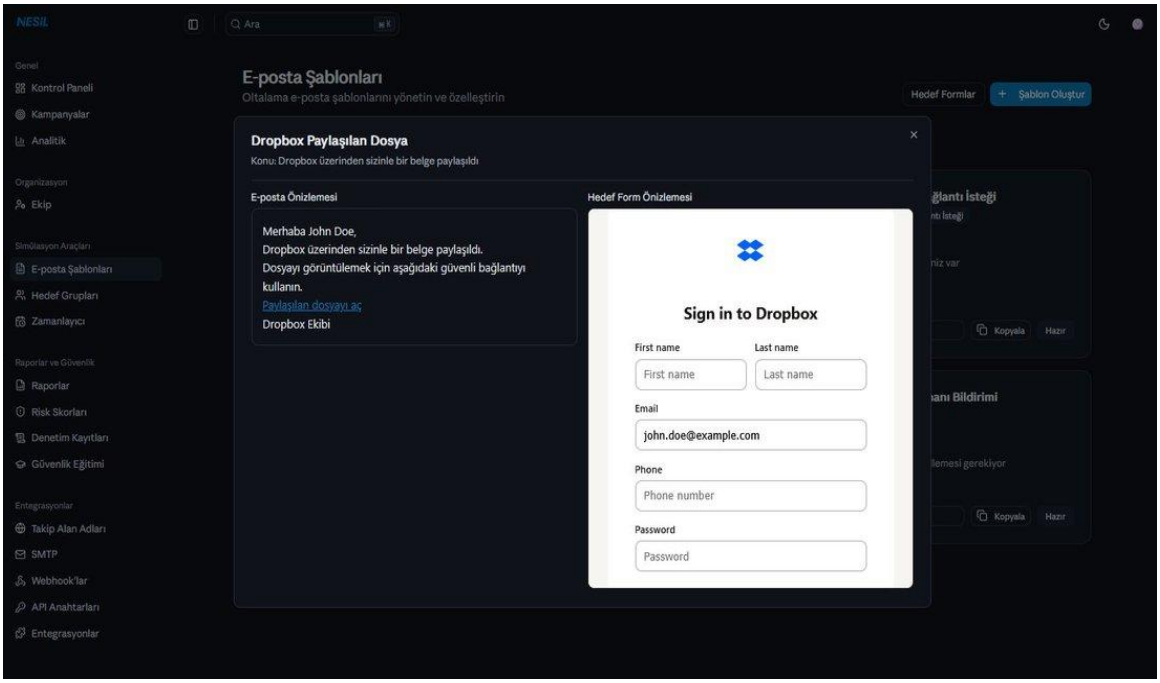



*The authentication page resembles LinkedIn's real design. It is a particularly attractive trap for career-building employees.*

- Who it is for: Sales, marketing, and senior managers — active LinkedIn users.
- Risk point: Since it is used in a corporate test about a non-corporate platform, providing an explanation in communications is recommended.

## 13.5 Dropbox Shared File

A scenario that comes with "A document has been shared with you via Dropbox," very effective especially in creative and marketing teams.

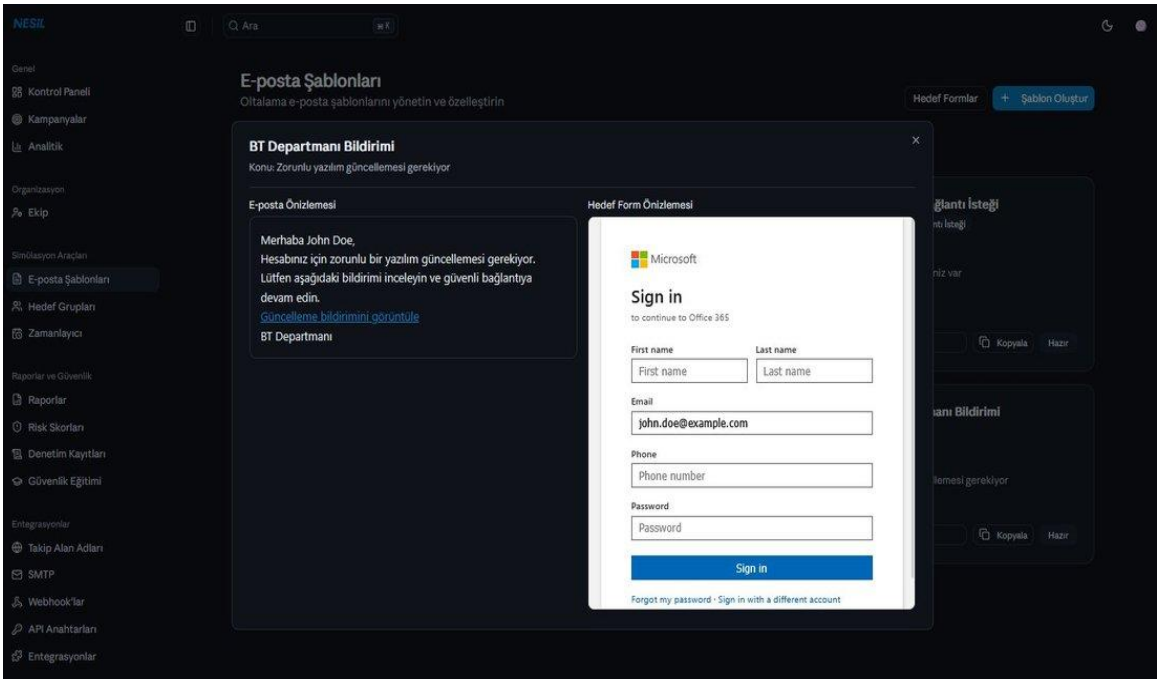



*The target form recreates the classic Dropbox login screen. The blue "Sign in to Dropbox" heading ensures the form is immediately recognized.*

- Who it is for: Organizations using Dropbox or similar file sharing services. Perfect for creative and agency teams.

## 13.6 IT Department Notification

"A mandatory software update is required" — a scenario that appears as an internal phishing email that looks like it came from the user's own IT team. Employees usually respond quickly to messages from the IT department — this template tests that trust.




*The email appears to be sent by the "IT Department." The target form resembles Microsoft's login screen and contains the text "to continue to Office 365."*

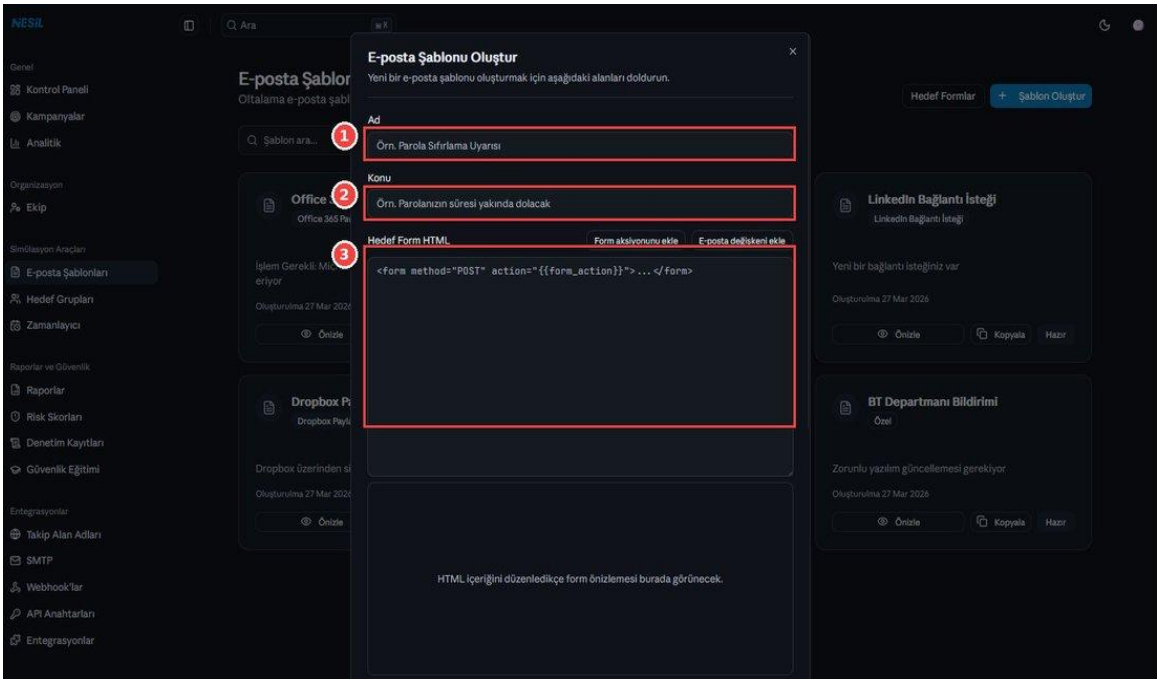
- Who it is for: Any organization — especially large companies with centralized IT services.
- Ethical note: Since it tests trust within the organization, it is recommended to run it with prior approval from senior management.

> **Trying multiple templates in sequence**
>
> Sending different scenarios to different departments is the fastest way to understand which areas your organization is most vulnerable in. For example: "IT Notification" to the finance department, "Dropbox" to the marketing team, "LinkedIn" template to the sales team — and then compare click rates.

# 14. Creating a Custom Template

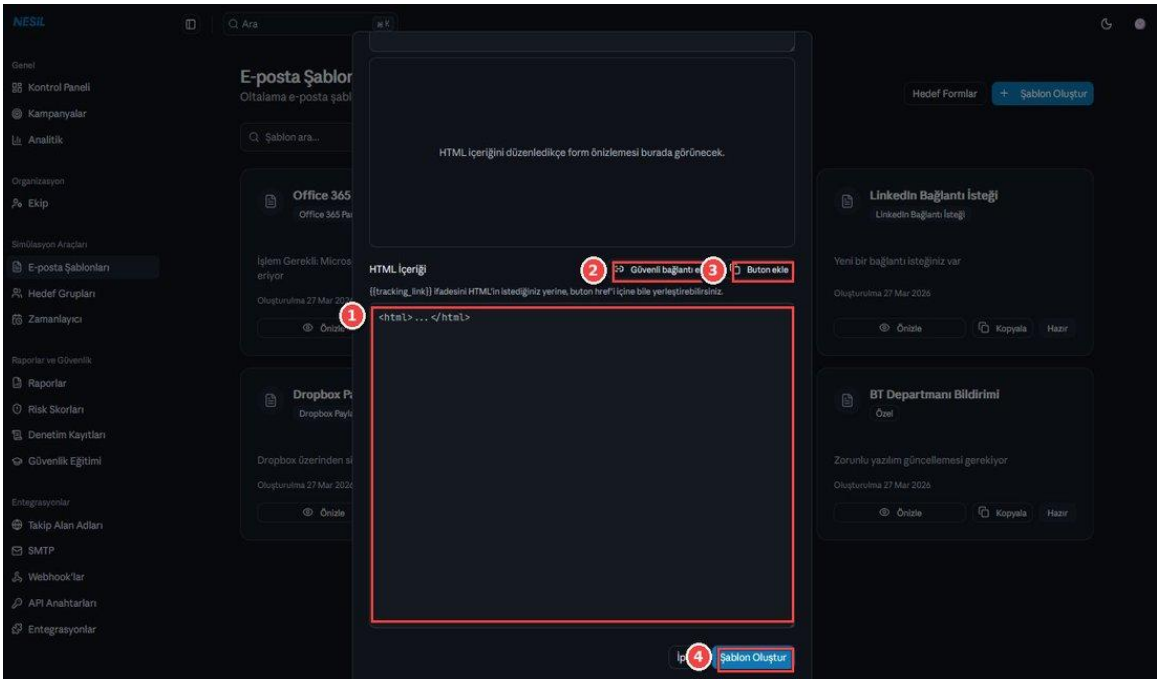
The ready-made gallery does not cover every scenario. You need to create a custom template for situations specific to your organization (e.g., a form mimicking your own HR portal, a special internal announcement). Nesil simplifies this with a two-panel editor: email information at the top, HTML content at the bottom.

## Upper section: basic information and form HTML




| | |
|---|---|
| 1 | **Ad** The internal name of your template. It appears with this name in the gallery and in the campaign selection list. E.g.: "Internal Payroll Alert". |
| 2 | **Konu** The email subject the target will see in their inbox. Should be a short sentence with a call to action. |
| 3 | **Target Form HTML** The HTML code of the form that will open when the user clicks the link. The system automatically replaces the {{form_action}} variable with the real tracking address. |

## Lower section: email HTML content




**1** **HTML Content** The actual email body. You can write rich HTML: headings, images, buttons.

**2** **Add tracking link** When you press the button, it inserts the {{tracking_link}} variable at the cursor position. This variable turns into a unique address for each target during sending.

**3** **Buton ekle** Inserts ready-made call-to-action button HTML code. You can edit the CSS styling if you wish.

**4** **Create Template** After filling in all fields, save it. The template drops into the gallery and becomes usable in every campaign.

## Variables you can use

- {{name}} — The target's name (if available).
- {{email}} — The target's email address.
- {{tracking_link}} — Unique tracking link. Turns into a different URL for each target during sending.
- {{form_action}} — Used only in the Target Form HTML; it is placed in the form's action attribute.

**HTML errors may be saved silently**

The system does not validate your HTML — unclosed tags or broken quotes may not be noticed until the campaign is launched.

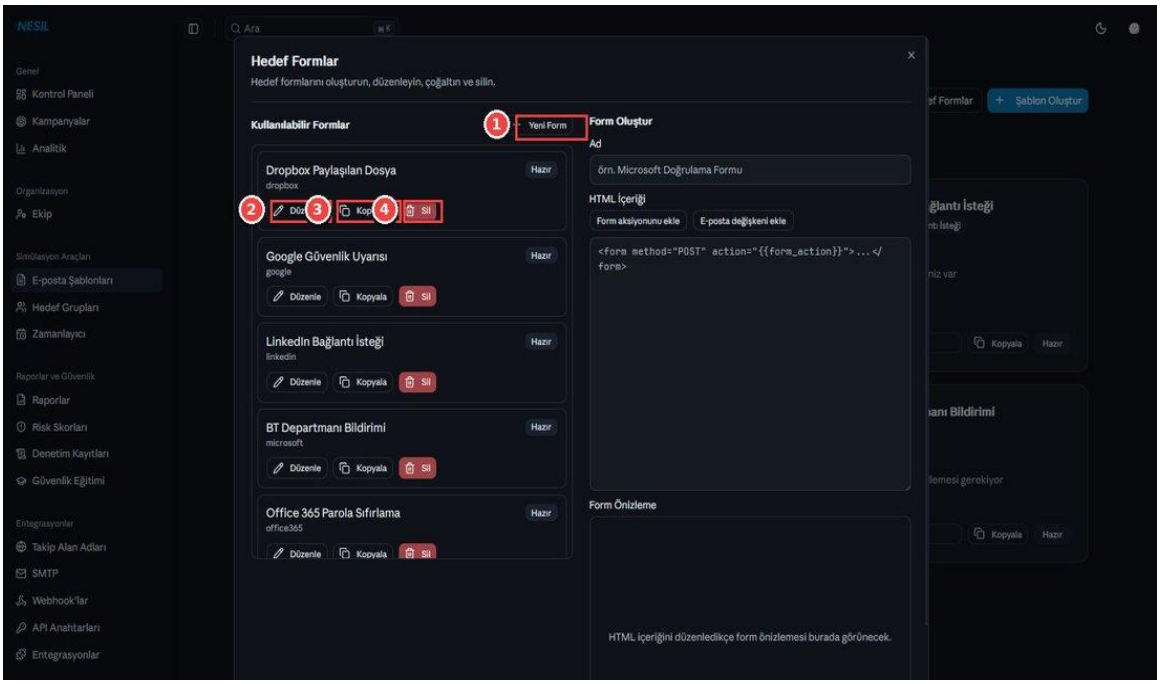
Safest approach: Before saving, check how the email and form look in the "Preview" area. If there is no preview, try sending a small test campaign to yourself.

**Start with Copy**

Rather than writing HTML from scratch, press the "Copy" button on a ready-made template in the gallery on the Email Templates screen and write over it. Both the variables (tracking_link, name) are in place and the HTML structure comes ready.

# 15. Target Forms

Target forms are the fake login pages that users encounter after clicking the phishing link. Nesil manages these in a module independent from email templates — so you can use the same form in multiple templates.




*Target Forms management panel. List of existing forms on the left, content editor of the selected form on the right.*

## Ekrandaki kontroller

**1** **New Form** Creates a target form from scratch. The editor on the right is cleared and you start editing a new form.

**2** **Edit** Opens a form from the list in the right panel. You can edit its HTML.

**3** **Kopyala** Clones the existing form. Use it to create a variant on top of a ready-made form without breaking it.

**4** **Sil** Permanently deletes the form. If there are campaigns using this form, the system warns you.

5 **Form Name** The internal name of the form. It will be selected by this name when creating a campaign.

6 **HTML Content** The visual and structural design of the form. The {{form_action}} special variable is filled by the system with where the form will be submitted.

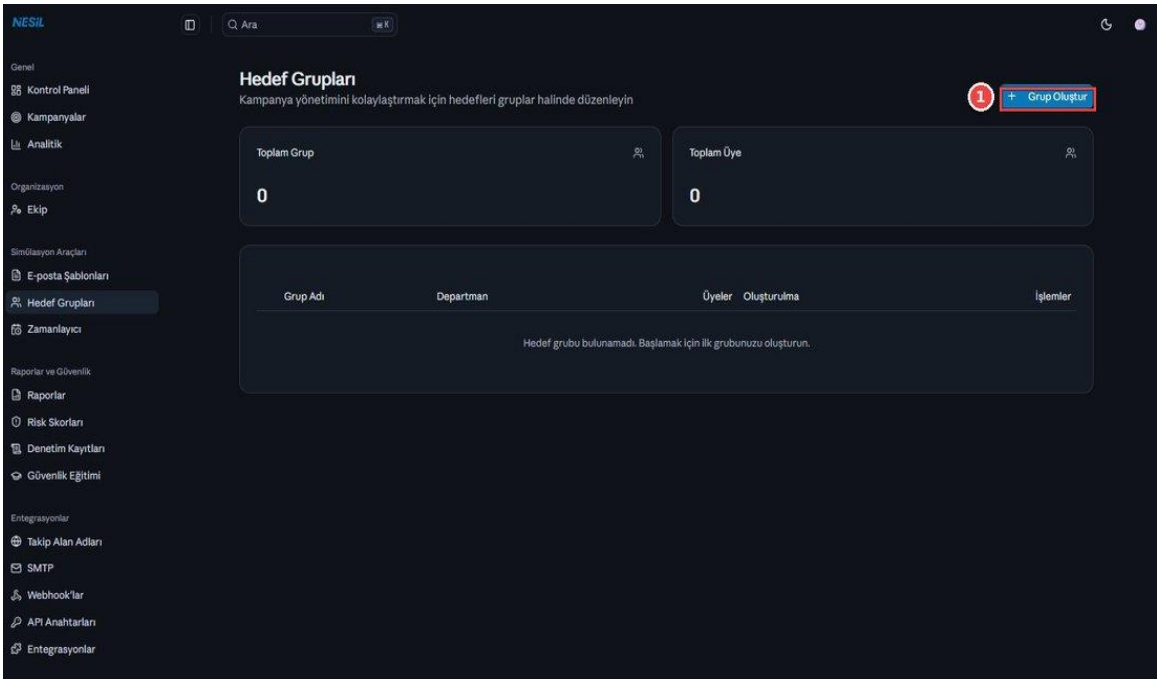
## Ready-made forms

- Dropbox Shared File — Dropbox login screen
- Google Security Alert — Google account login form
- LinkedIn Connection Request — LinkedIn login screen
- IT Department Notification — Microsoft / Office 365 login
- Office 365 Password Reset — Microsoft password confirmation

> **Email and form matching**
>
> It is critical for the scenario contained in an email template to be consistent with the visual of the target form. If an email saying "A document came from Dropbox" opens a Microsoft login form when clicked, the user's suspicion immediately increases.
>
> Nesil knows this and warns by automatically resetting the form selection when the template is changed in the create campaign modal.

# 16. Target Groups

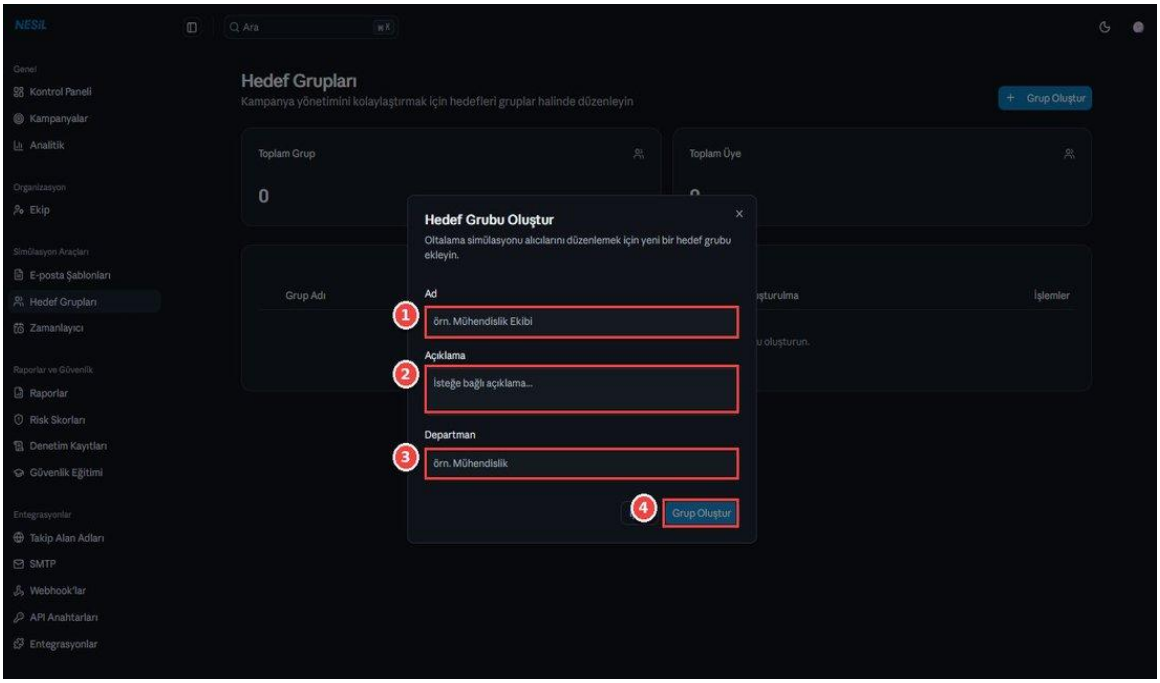
Target groups allow you to save lists of people you will use repeatedly in campaigns. For example, create a "Sales Department" group and add 20 people to it; you can import this list with a single click for each new sales campaign. It is also the basis of department-level risk analysis — the group name is used as the department in reports.




*Empty Target Groups screen. Two summary cards (Total Groups / Total Members) and a list table below.*

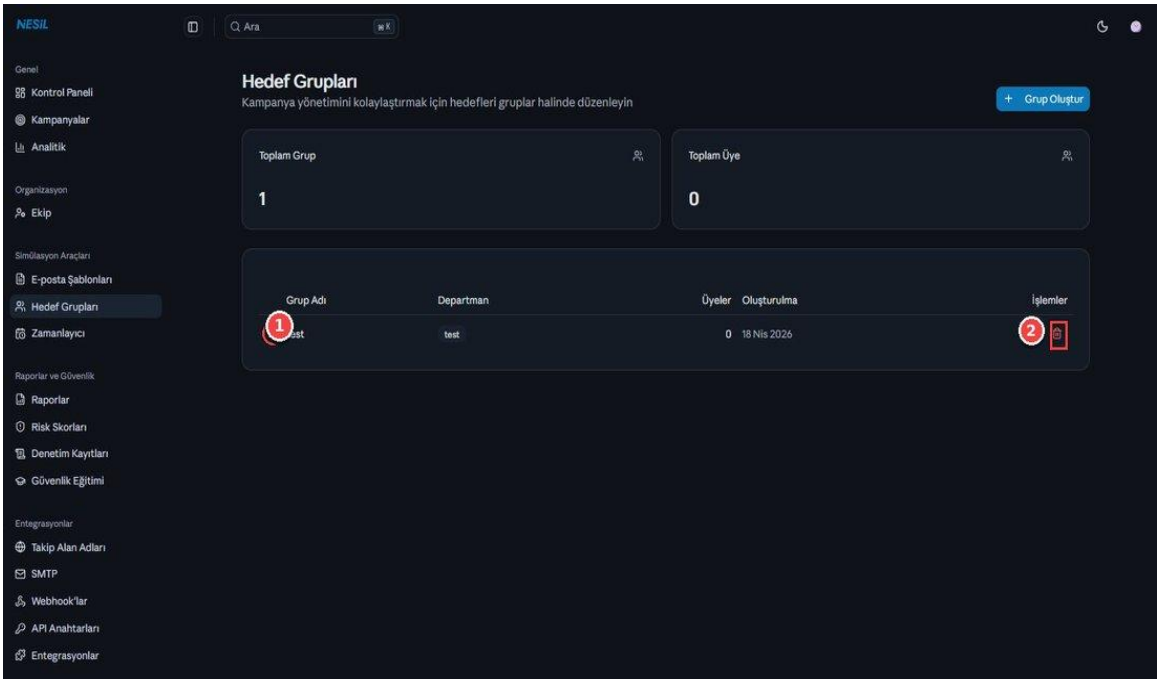
## Creating the first group

1 **Click the Create Group button** Open the modal with the blue button in the top right.

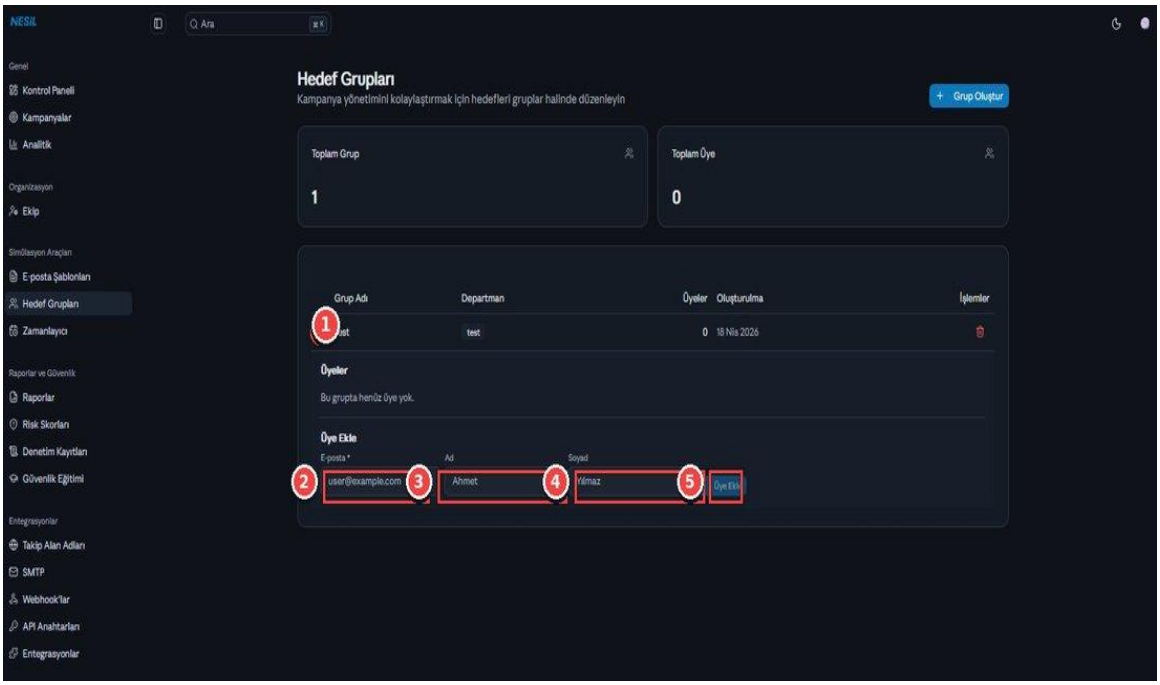



| | |
|---|---|
| 1 | **Ad** The display name of the group. E.g.: "Sales Department", "New Starters 2026". |
| 2 | **Description (optional)** Who makes up this group, what purpose does it serve? Free text. |
| 3 | **Departman** Which department this group will be counted as in risk reports. A single word is sufficient (e.g., "finance", "hr"). |
| 4 | **Create Group** The group is created and starts appearing in the list. |

## Adding members to a group




*List view after the group is created. You can expand the group with the arrow (>) at the far left of its row.*




*An expanded group. The member addition form appears at the bottom.*

| | |
|---|---|
| 1 | **Expand arrow** Click the arrow icon at the far left of the group row. The group detail expands downward. |

2 **E-posta** The email address of the person to be added. Required field.

3 **Ad** The person's name. Appears in the {{name}} variable in emails.

4 **Soyad** Last name. Optional.

5 **Add Member** Adds the person to the group. Fields are automatically cleared; you can add several people one after another.

**Set up groups with a department logic**

The department field is used as an independent axis in the Reports and Risk Scores screens. So keeping the "sales" group separate rather than merging it with "marketing" increases your reporting power.

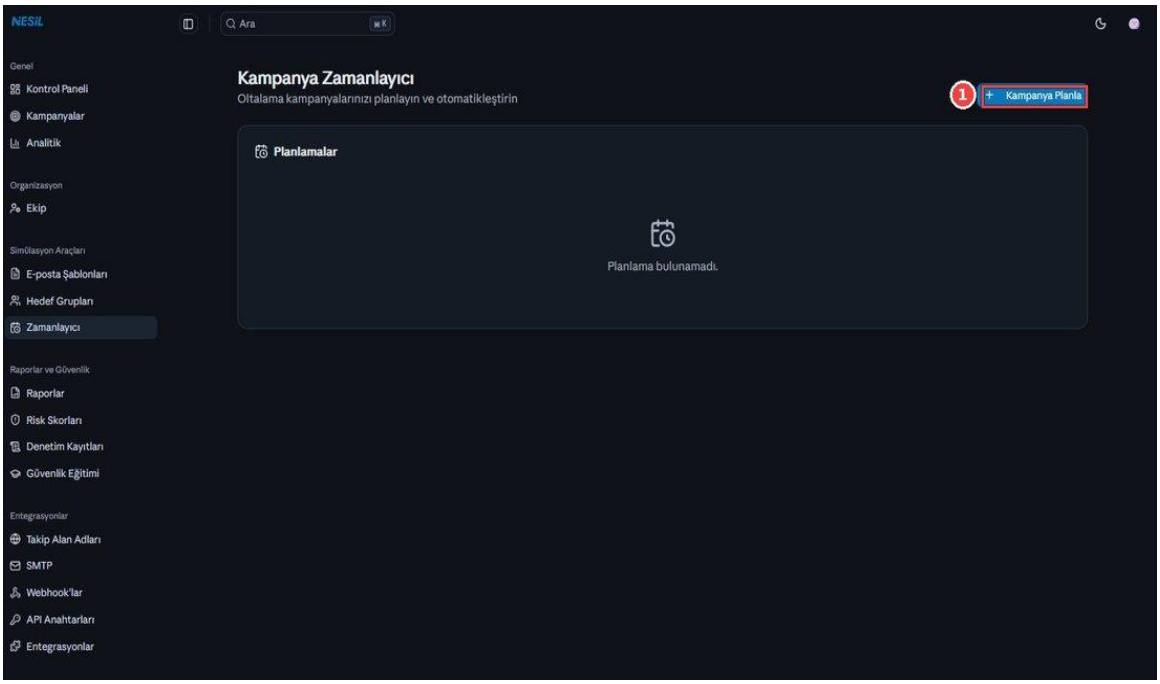
Set the naming standard from the start: all lowercase, put hyphens between words (e.g., "information-technology"). Changing it later is difficult.

**No CSV upload?**

This screen focuses on adding individual members. If you want to do bulk uploading, it is more practical to first add targets in bulk to the campaign and then keep those targets under a group.

# 17. Scheduler

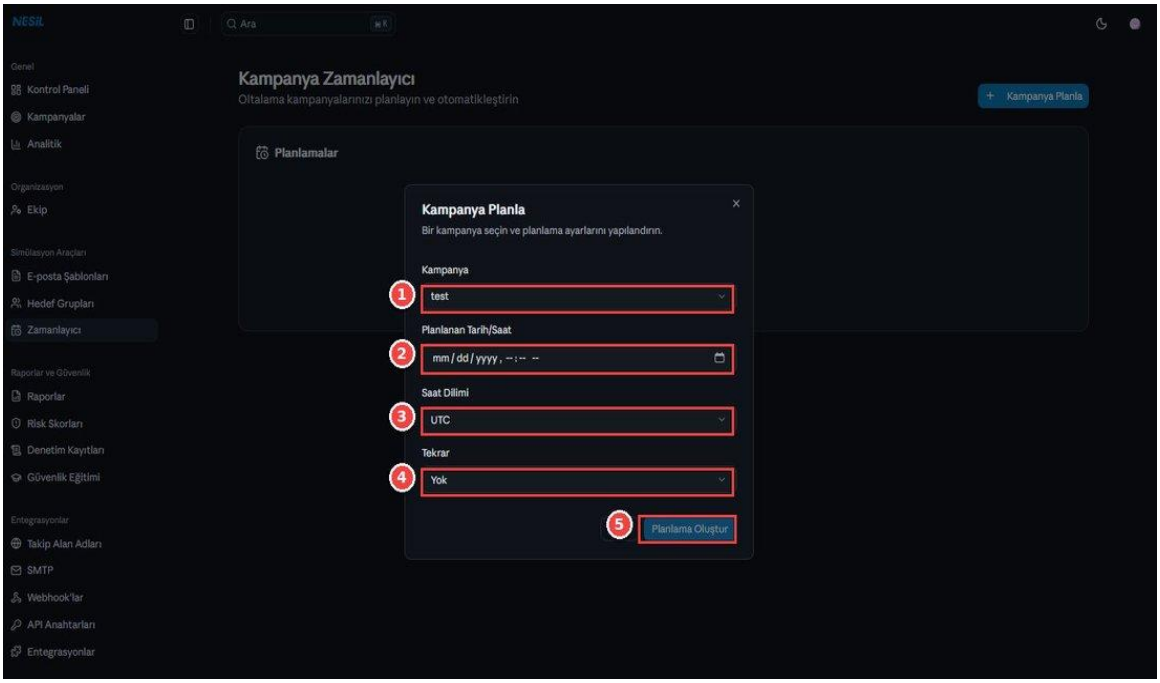
The Scheduler lets you run campaigns automatically at a specific date and time instead of launching them manually. It is ideal for strategic moments such as catching office rush hour at 09:30 in Turkey or testing afternoon distraction on a Friday.




*Empty Scheduler screen. No campaigns scheduled yet.*

## Creating a schedule

1 **Click the Schedule Campaign button** The button in the top right opens the modal.



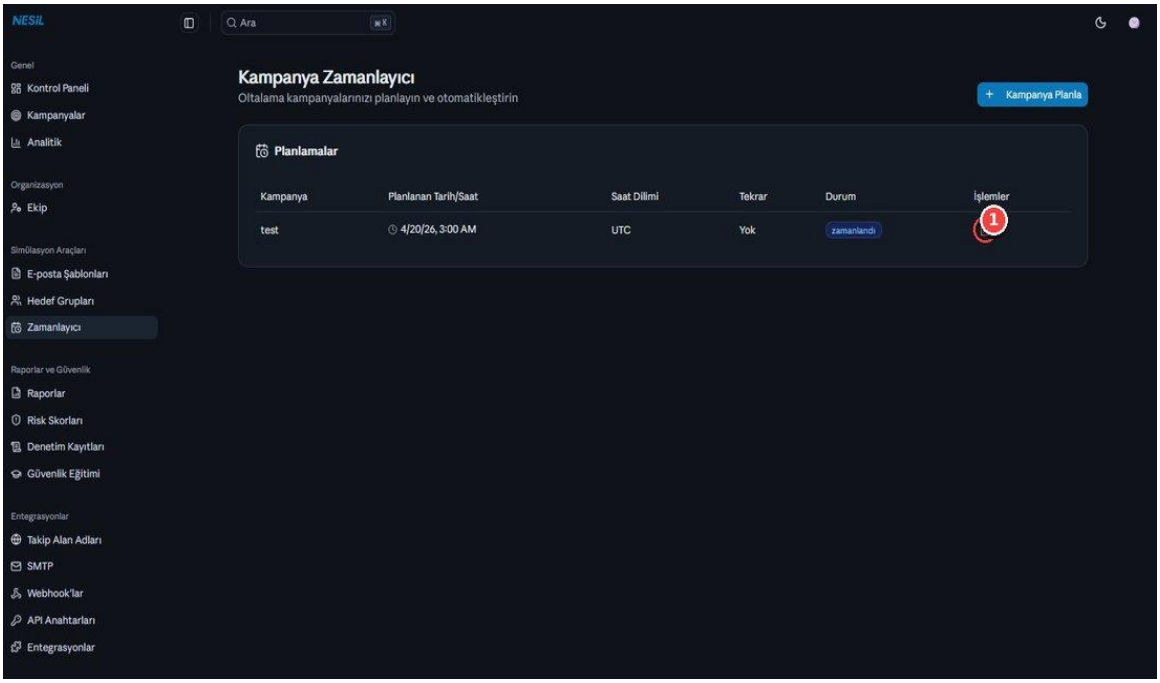

**1** **Campaign** Select one of the campaigns you created previously. You can select from those in Draft status.

**2** **Planlanan Tarih/Saat** The moment sending will start. You can easily set it from the calendar using the date picker.

**3** **Saat Dilimi** Which time zone the schedule will be valid in. Default is UTC; select "Europe/Istanbul" or UTC+3 for Turkey.

**4** **Tekrar** Whether the campaign runs weekly, monthly, or once. If "None" is selected, it is launched only once.

**5** **Create Schedule** The schedule is saved and drops into the list.




*A scheduled campaign. The status badge shows "scheduled." It automatically switches to "active" at the time of sending.*

### Beware of time zone errors

Confusion between UTC and local time can cause campaigns to run hours earlier or later than expected. If you want to launch at 14:00 in Turkey, make sure to select the Europe/Istanbul time zone from the dropdown.

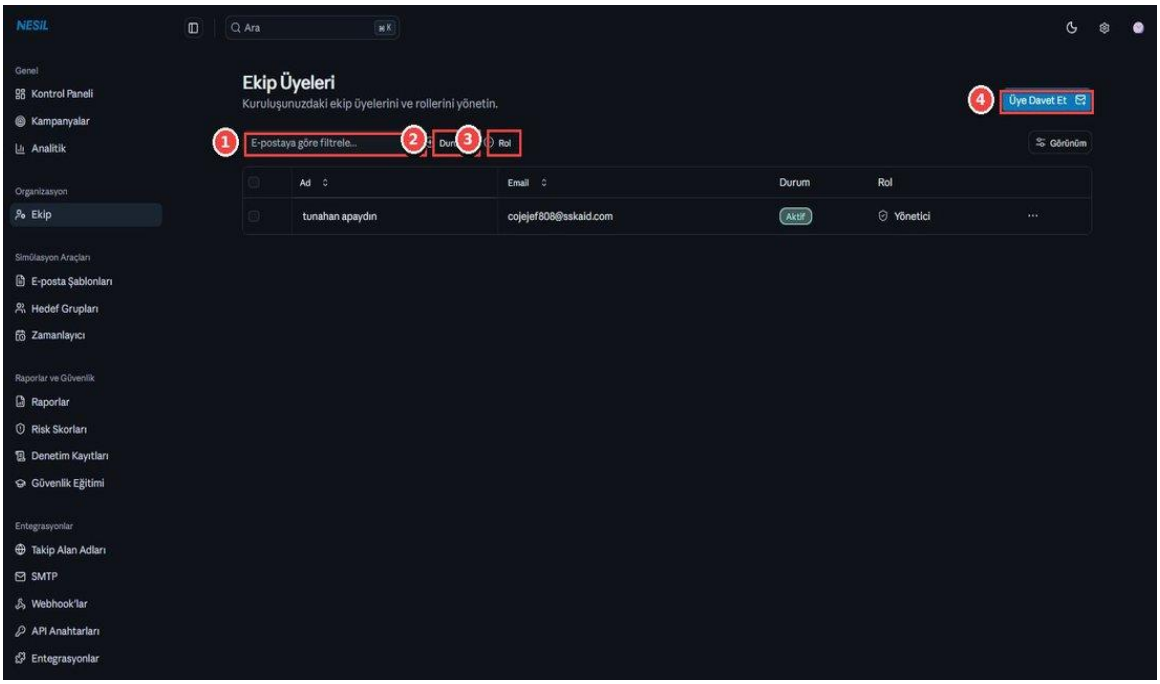
There is no daylight saving time change in Turkey (fixed UTC+3); if you are working with overseas teams, check their time zone as well.

### Canceling the schedule

In the list view, there is a red delete icon at the far right of each row. Press it to cancel the schedule. If a campaign has already been launched, cancellation does not stop it — it only prevents new submissions.

# 18. Team Management

The Team menu comes into play when more than one person from your organization needs access to the platform. From here you can invite new members, assign their roles, and manage the status of their accounts.




*Team Members screen. The list of existing members, filters, and the "Invite Member" button are in the top row.*

## Ekrandaki kontroller

**1** **Filter by email** Use this to quickly find a specific person as the list grows.

**2** **Durum filtresi** Narrow the list by Active, Inactive, Invited, or Suspended status.

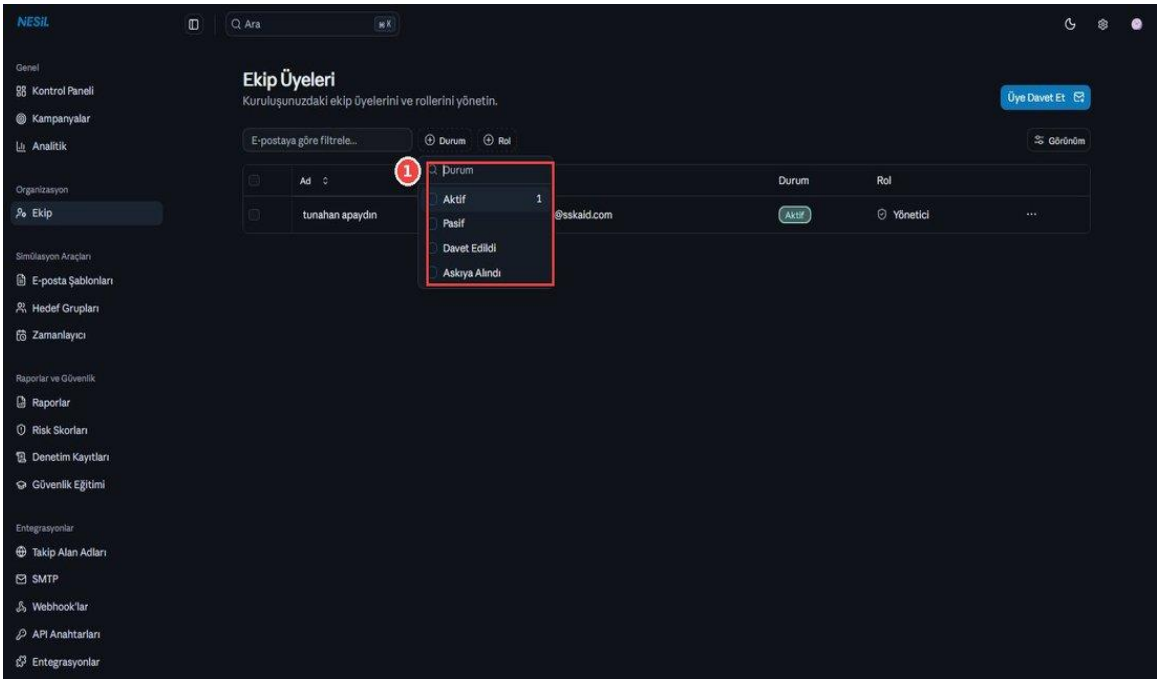
**3** **Rol filtresi** Filter by Administrator, Manager, or Member role.

**4** **Invite Member** Opens the modal to invite a new user.

**5** **Row actions (…)** Menu for member-specific operations such as changing role, suspending, or deleting.

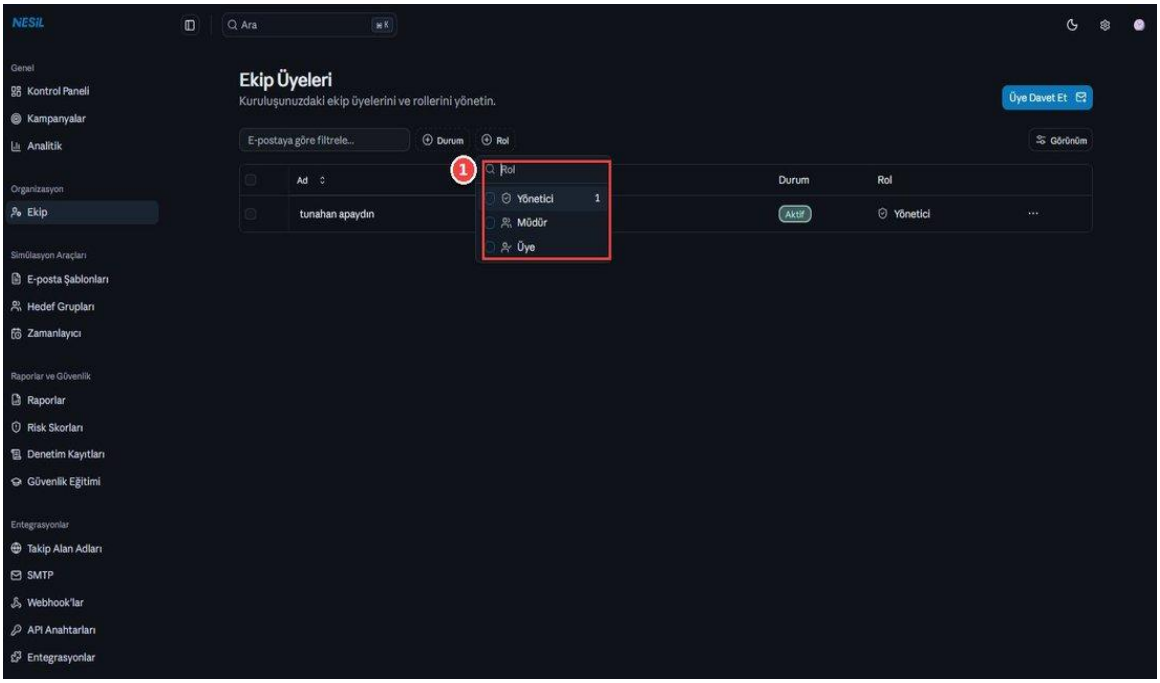
6 **View** Select / hide table columns. Useful for a compact view in large teams.

## Status filter options



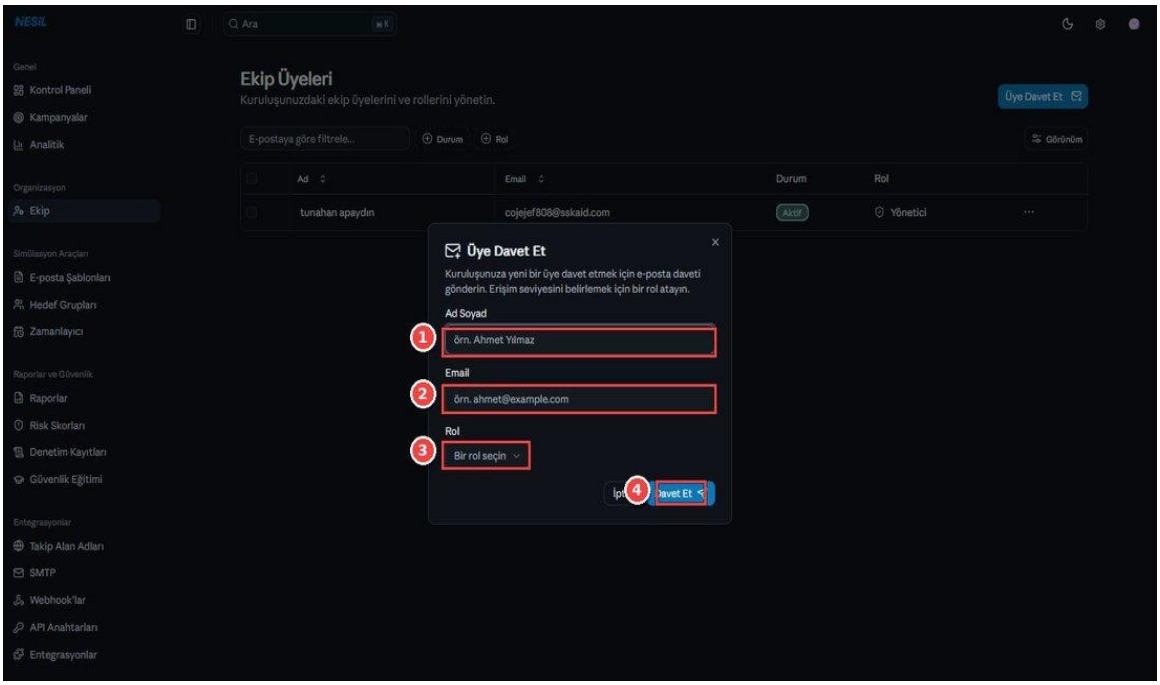

- Active — Normally functioning account.
- Inactive — Manually disabled; cannot log in.
- Invited — Invitation sent but not accepted.
- Suspended — Temporarily frozen for security reasons.

## Role filter options




- Administrator — The top role with access to all settings and billing, can change roles.
- Manager — Broad authority over campaigns and team; no billing access.
- Member — Can only view and edit campaigns assigned to them.

## Inviting a new member




**1** **Ad Soyad** The invited person's name. Appears in the {{name}} variable in email templates.

2 **Email** The email address to which the invitation link will be sent.

3 **Rol** Choose from Administrator / Manager / Member.

4 **Davet Et** An invitation email is sent. The account becomes active when the user accepts the link and creates their password.

**Distribute roles carefully**

The Administrator role is very powerful — it grants access to critical areas such as billing, SMTP, and API keys. Give Administrator to no more than 1-2 people within the organization.

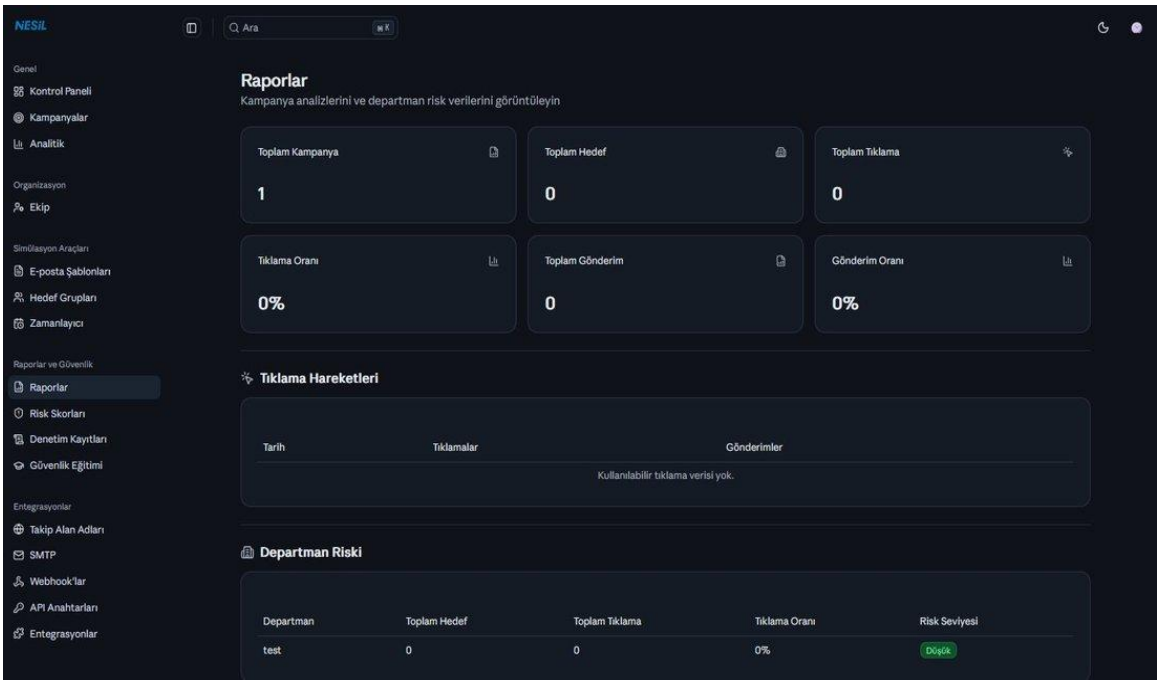
Manager is ideal for everyday campaign managers, and Member is ideal for external teams working on assignment.

**Invitation may expire**

The invitation email becomes invalid after a certain period of time. If the user does not accept in time, they remain listed as "Invited" and the invitation needs to be renewed. Use the "Resend Invitation" option from the row actions menu.

# 19. Reports

The Reports screen is the management view showing campaign and department performance together. While the Dashboard and Analytics provide more "instantaneous" views, Reports reveals the long-term risk profile of your organization.




## Three main areas

1 **KPI strip (6 cards)** Total Campaigns, Targets, Clicks, Click Rate, Submissions, and Submission Rate. Having six metrics together provides a "single view" advantage in reporting.

2 **Click Activity** Shows the number of clicks and submissions over time. The table updates live when new data arrives.

3 **Departman Riski** Each department's (i.e., each Target Group's) own click count, total targets, and calculated risk level (Low / Medium / High) are here.

## The difference between click rate and submission rate

The two metrics can easily be confused:

- Click Rate — What percentage of targets in the campaign clicked the phishing link? This is the "initial awareness" indicator.
- Submission Rate — How many targets filled out and submitted the fake form? This is the "actually took the bait" indicator.

> **Reading the two metrics together**
>
> If the click rate in a campaign is 20% but the submission rate is 3%: most users clicked the link and examined it curiously but stopped thinking "this form is suspicious." This is a good signal; the "pause" reflex can be improved with training.
>
> The opposite, click 5% but submission 5%, is more alarming — everyone who clicked filled out the form. This segment requires urgent training.

## How is the department risk level calculated?

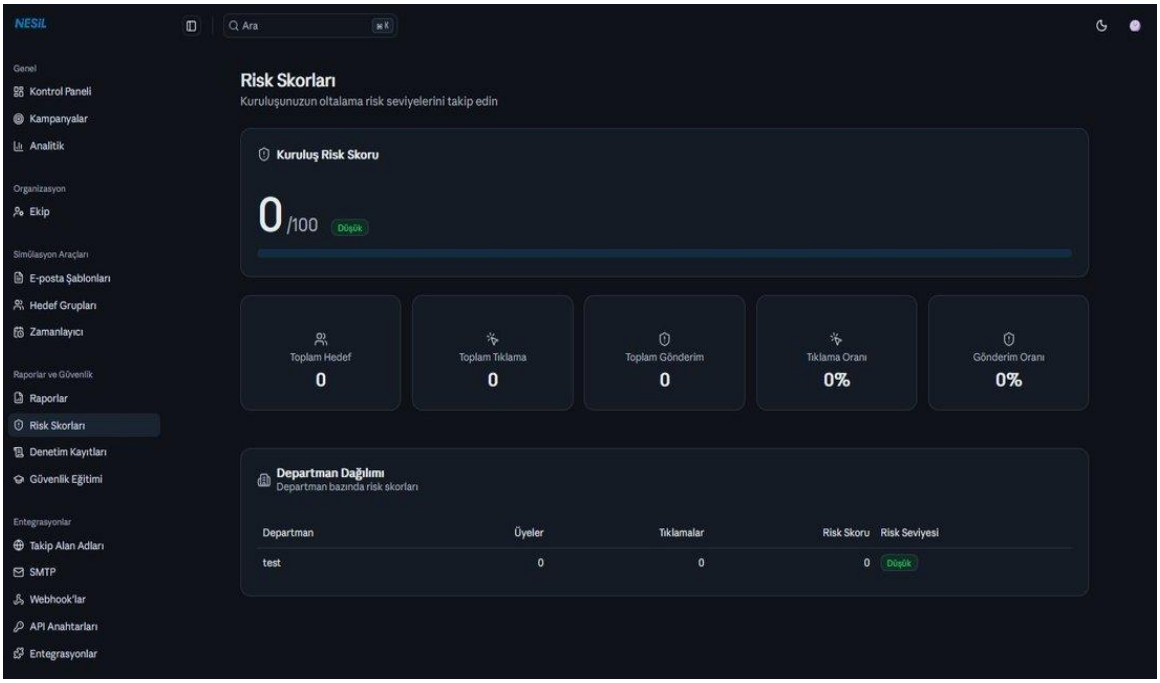
The system automatically assigns a level based on the department's click rate:

- Low — Click rate below 5%.
- Medium — Between 5%–15%.
- High — Above 15%.

These thresholds may change over time to be specific to your organization; use them as initial values.

# 20. Risk Scores

Risk Scores summarize your organization's security awareness with a single number derived from all campaign results. This score is between 0-100; a lower score is a good sign.




## Organization Risk Score

The large number at the top shows the overall risk level of your organization. The colored band behind it visually indicates which range your score is in.

- 0-20: Low risk (green)
- 21-50: Medium risk (yellow)
- 51-80: High risk (orange)
- 81-100: Critical risk (red)

## Detail metrics

Five summary cards in the bottom row: Total Targets, Total Clicks, Total Submissions, Click Rate, and Submission Rate. These values are calculated for the entire organization.

## Department Distribution

Shows a separate row for each department: member count, click count, calculated risk score, and risk level badge. This list clearly shows which departments need priority training investment.

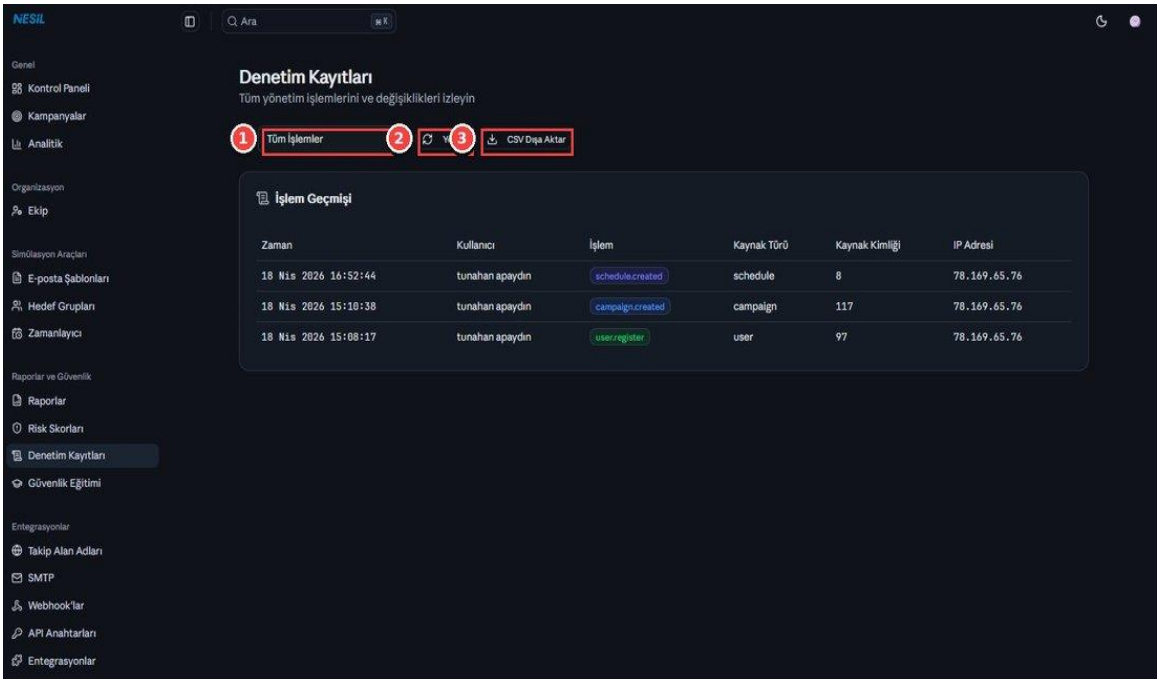
### Tracking the risk score over time

The score is valuable as a trend rather than a single data point. If you get the same score three months in a row, your awareness efforts are insufficient; a 20% drop from the previous quarter is proof that your strategy is working.

Saving the chart once a month and comparing over time when presenting to management is a powerful practice.

# 21. Audit Logs

Audit Logs record every administrative action performed on the platform in an immutable log. When a user creates a campaign, changes a setting, or deletes a target — all of it is written here. The answers to the "what happened, who did it, when?" questions required by compliance standards such as KVKK, ISO 27001, and GDPR are found on this screen.




## Ekrandaki kontroller

1 **Action filter** Narrow the list by selecting a specific event type (e.g., only "campaign.created") instead of "All Actions".

2 **Yenile** Use this to instantly pull the latest events — the page does not auto-refresh.

3 **Export CSV** Downloads all events matching the selected filter as a CSV. Very useful for archiving during compliance periods.

4 **Action History table** Event list with columns for time, user, action badge, resource type, resource ID, and IP address.

## Common action types

- user.register — New user registration
- user.login — Successful login
- campaign.created — New campaign created
- campaign.started — Campaign launched
- campaign.deleted — Campaign deleted
- schedule.created — Scheduled sending planned
- target.added — Target added to campaign
- smtp.updated — SMTP settings changed
- api_key.created — New API key generated

**KVKK / ISO 27001 compliance support**

The audit log is one of the first documents a compliance auditor will request from your organization. Run the CSV export feature periodically (e.g., at the end of each quarter) and back it up — having a copy outside the platform is advisable.

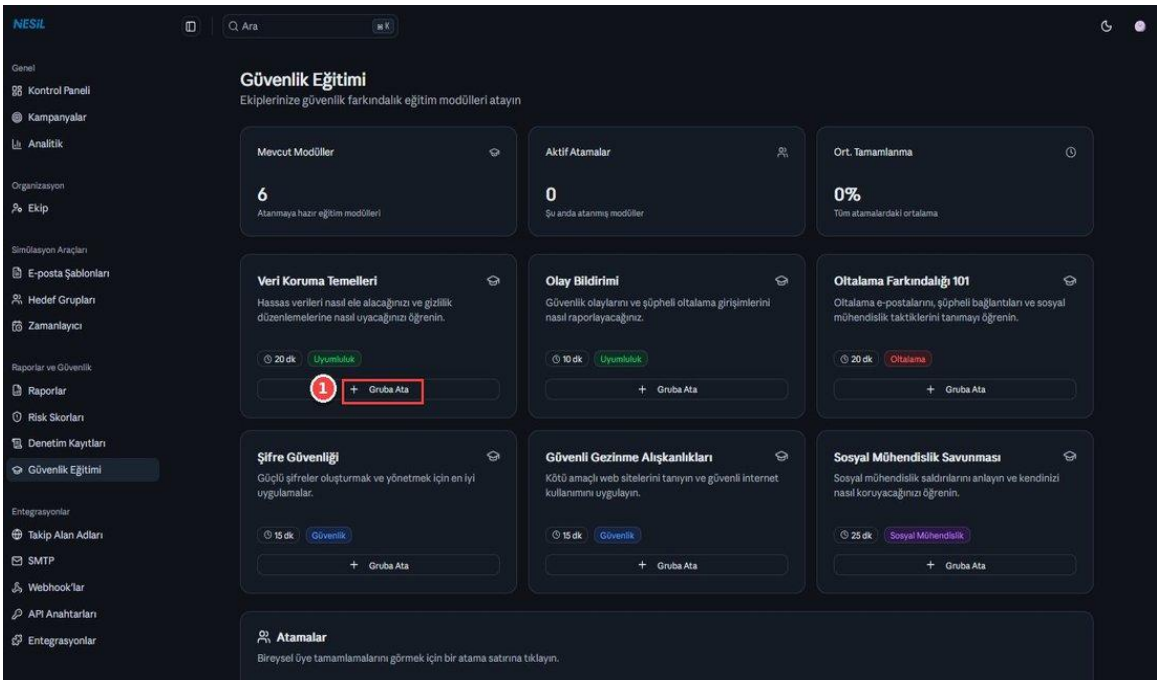
The "immutable" nature of the log means existing records cannot be edited later; this feature is the foundation of evidence.

**The question of which IP it came from**

Every event records which IP address it was performed from. If a VPN or proxy is used in your organization, this IP may be fixed. If you see a suspicious action, share the IP with your IT team to verify who was connected from that session.

# 22. Security Training

A phishing drill is only half of the test. The other half is giving the right training to users who took the bait (and to all employees in general), both after the drill and proactively. The Security Training menu allows you to assign ready-made training modules to your teams.




*Security Training main screen. Three summary cards and assignable module cards below.*

## Top KPI strip

- Available Modules — The number of ready-made modules you can use (6 by default).
- Active Assignments — The number of assignments currently assigned to a group and still ongoing.
- Avg. Completion — Average completion percentage of assignments.

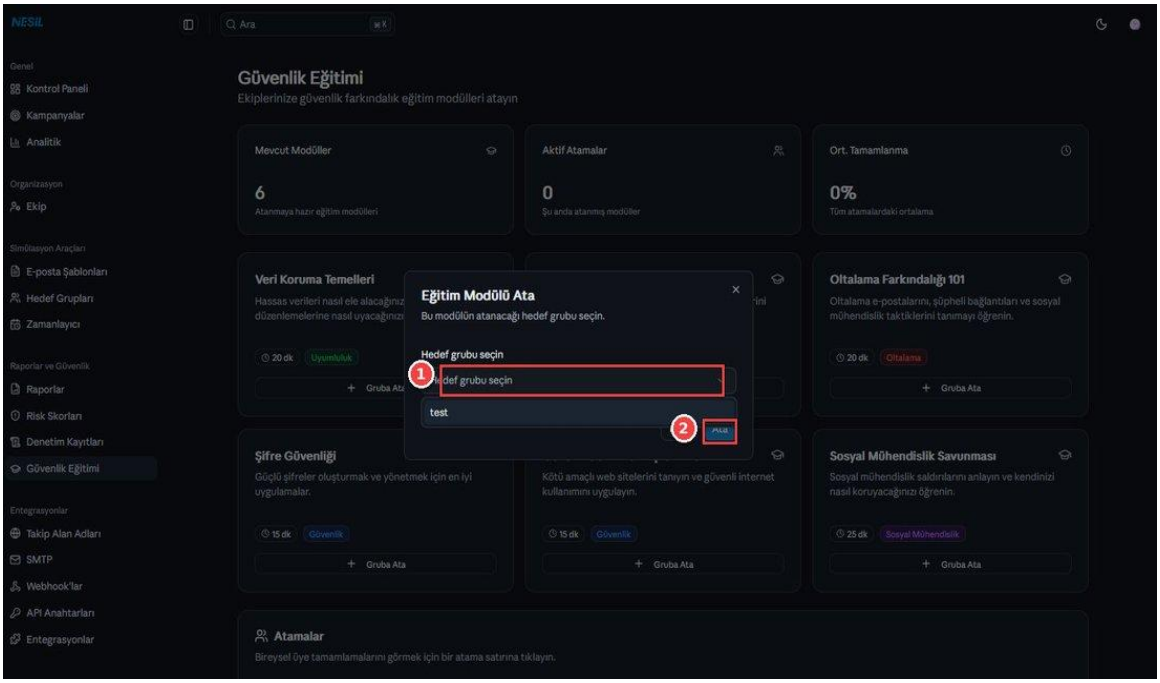
## Ready-made modules

- Data Protection Fundamentals — Handling sensitive data and privacy regulations (20 min, "Compliance" tag).
- Incident Reporting — How to report security incidents (10 min, "Compliance").
- Phishing Awareness 101 — Suspicious links and social engineering tactics (20 min, "Phishing").
- Password Security — Creating and managing strong passwords (15 min, "Security").
- Safe Browsing Habits — Internet usage and recognizing malicious sites (15 min, "Security").

- Social Engineering Defense — Recognizing psychological manipulation techniques (25 min, "Social Engineering").

## Assigning a module to a group

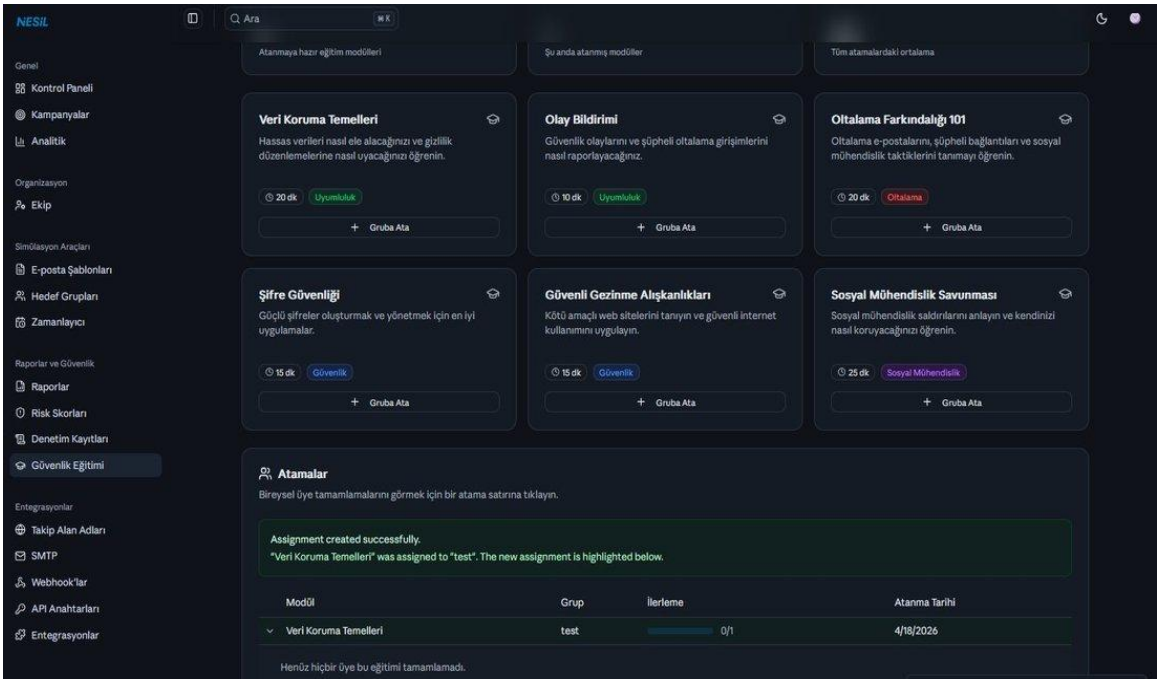
1 **Press the "Assign to Group" button on the relevant module's card** This button is located at the bottom of each module card.




1 **Select a target group** Select one of your previously created groups from the dropdown list.

2 **Ata** The module is assigned to all members of that group. The system automatically sends each member an email containing a training launch link.

## Monitoring assignments




*Post-assignment view. A green confirmation message appears at the bottom of the page, followed by an assignment row.*

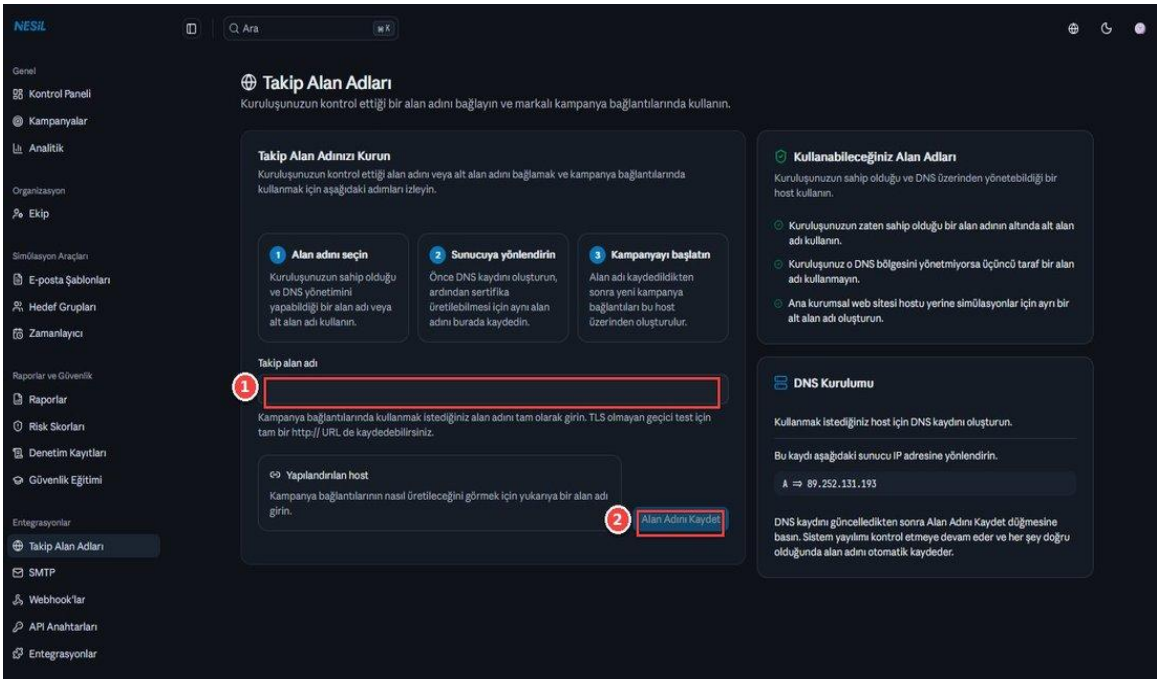
Each assignment row shows:

- Module — The assigned training name
- Group — Which group it was assigned to
- Progress — Number of members who completed / total members, like "0/1, 2/5"
- Assignment Date — The date the assignment was made

> **Best time for training assignment**
>
> Immediately after a phishing simulation, assign the relevant module to those who clicked. Sending "Phishing Awareness 101" to users who took the bait immediately reinforces behavior-based learning.
>
> Making at least one "Data Protection Fundamentals" assignment to all employees annually makes your job easier during compliance audits.

# 23. Tracking Domains

By default, Nesil generates tracking links in the "nesil.ai/p/..." format. However, in corporate campaigns, having these links appear associated with your brand (e.g., "mail-security.yourcompany.com/p/...") increases both credibility and filter bypass. This section explains how to connect your own domain.




## Connecting a domain in three steps

1 **Choose a domain** Use a domain or subdomain that your organization owns and can manage DNS for. (Step 1 box on the left side of the panel.)

2 **Point to the server** First create the DNS record; then register the same domain here so a certificate can be generated. (Step 2 box.)

3 **Launch the campaign** After the domain is registered, new campaign links are generated via this host. (Step 3 box.)

## Fields on the screen

1 **Tracking domain input** Write the domain name you want to use exactly. An http:// URL can also be registered for temporary testing without TLS.

2 **Save Domain** When you press the button, the system checks the DNS, and if everything is correct, the domain is automatically activated.

The "DNS Setup" panel on the right side of the page shows which IP your A record needs to point to — the example values are automatically generated by the system for each organization.

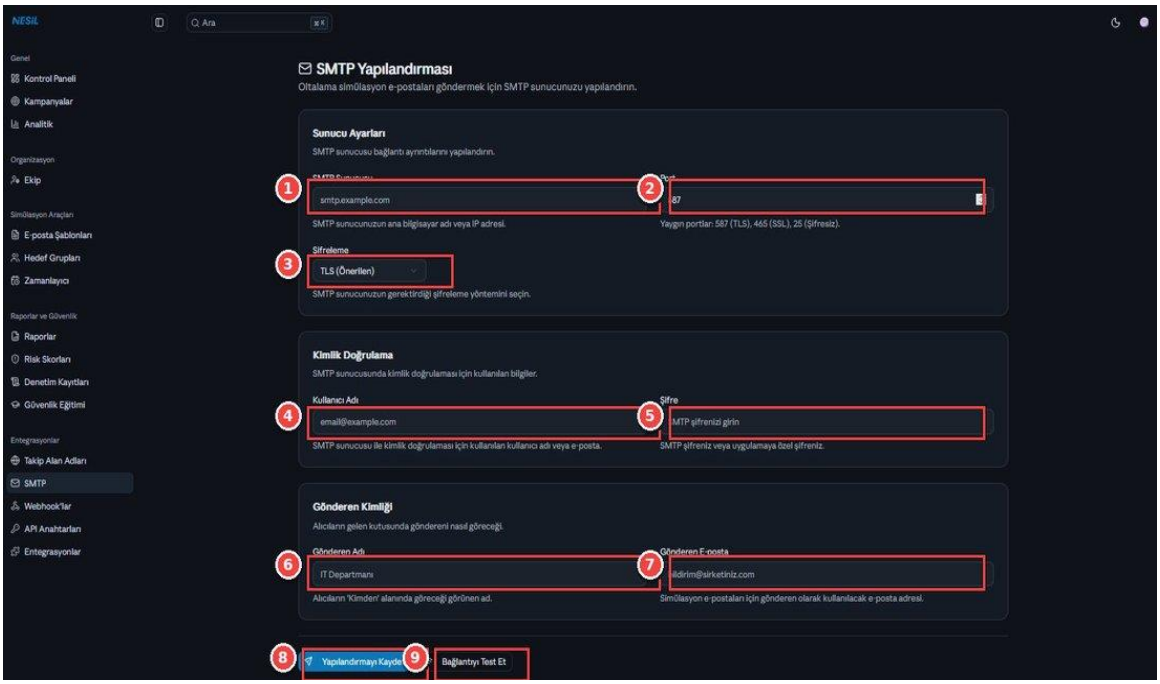
## Choosing the right host

- Use a subdomain under a domain your organization already owns (e.g., if yourcompany.com is your domain, use mail-check.yourcompany.com).
- Do not use a third-party domain if your organization does not manage that DNS zone.
- Create a separate subdomain for simulations instead of using the main corporate website host — this eliminates the risk of affecting the live site.

> **DNS propagation takes time**
>
> After adding a DNS record, propagation can sometimes take a few minutes, sometimes hours. Do not worry if the system gives an error on the first check — wait a while and press the "Save Domain" button again.
>
> A certificate is automatically generated after registration; no extra step is required.

# 24. SMTP Configuration

For your phishing simulation emails to land in the inboxes of targets, they need to be sent via an SMTP server. Nesil allows you to connect your own sending server (or a service like Sendgrid, AWS SES, or Mailgun).




## Server Settings section

**1** **SMTP Sunucusu** The hostname or IP address of the server to send from (e.g., smtp.sendgrid.net, mail.yourcompany.com).

**2** **Port** Common ports: 587 (TLS) — recommended; 465 (SSL); 25 (Unencrypted) — usually blocked.

**3** **Encryption** Choose from TLS (recommended), SSL, or unencrypted. Use TLS for secure sending.

## Authentication section

4 **Username / Email** The username or email used to log in to the SMTP server.

5 **Password** Your SMTP password or application-specific password. Note: this area is very sensitive.

## Sender Identity section

6 **Sender Name** The name recipients will see in the "From" field of their inbox. E.g.: "IT Department", "HR Security".

7 **Sender Email** The sender address. Must be an address that your SMTP's DKIM/SPF has approved.

## Saving and testing

8 **Save Configuration** Girdiklerinizi saklar.

9 **Test Connection** The system opens a test connection to the server using the settings and notifies you of the result.

**No email is sent to a real user**

"Test Connection" does not send a real email — it only connects to the SMTP server and authenticates. For a real delivery test, it is recommended to create a small test campaign and send it to your own email.

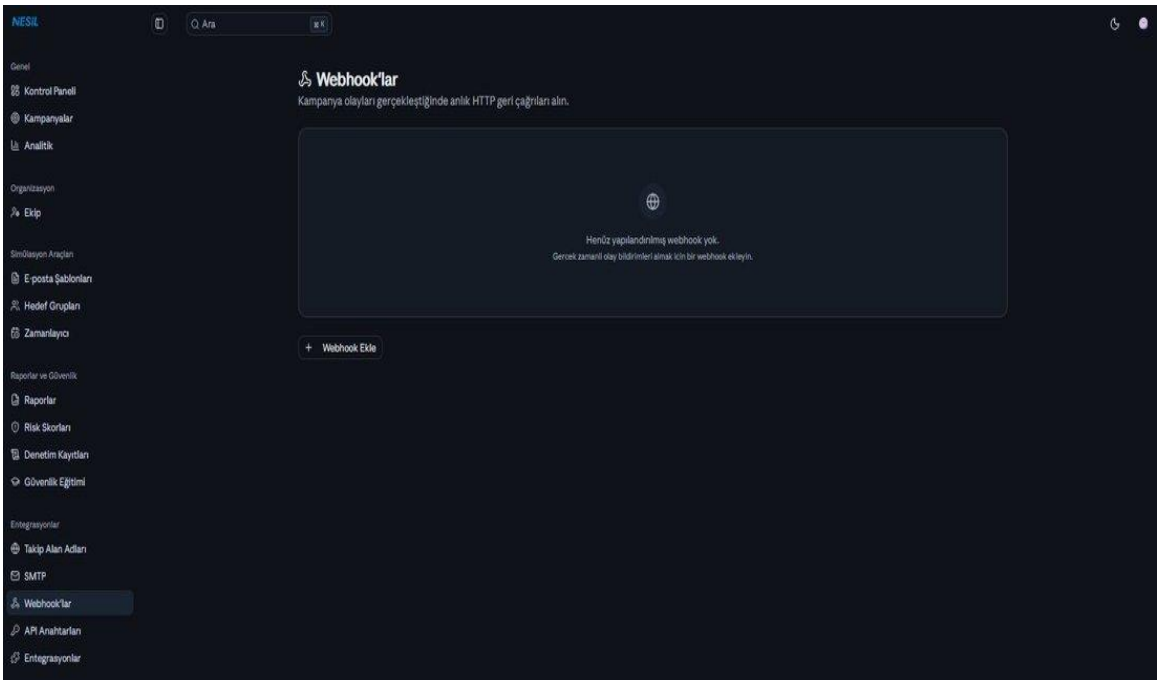
**DKIM, SPF, DMARC are important**

The DKIM and SPF records of the sender email address you use must be correctly configured — otherwise emails will end up in the spam folder of targets and your drill will make incomplete measurements.

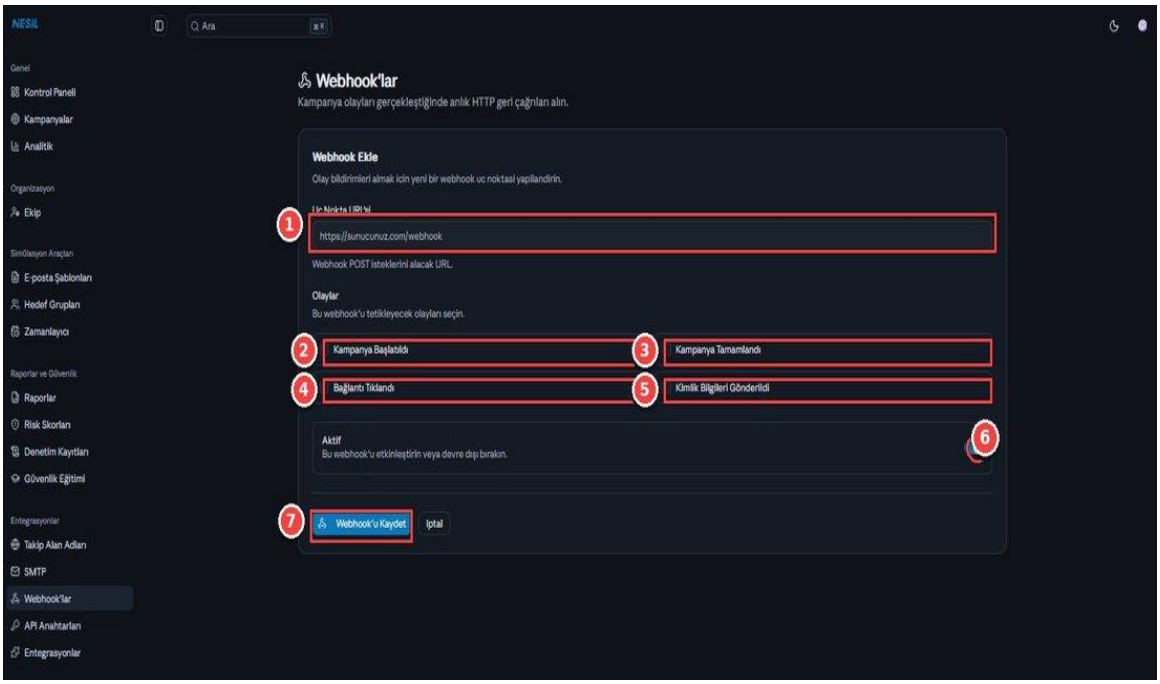
> Ask your IT team to verify the DNS records. Services like Sendgrid / Mailgun provide you with their own DKIM/SPF records.

# 25. Webhooks

Webhooks allow you to transmit what is happening on the platform to other systems in real time. Automations such as notifying your SIEM when a campaign is launched, or opening a record in your ticketing system when a target clicks, are set up with webhooks.




*Empty Webhooks screen. You can start the first configuration with the "Add Webhook" button.*




*A new webhook addition form.*

## Form fields

1. **Endpoint URL** The URL that Nesil will send a POST request to. E.g.: https://yourserver.com/webhook.

2. **Campaign Launched** Select the event to be triggered when the submission flow starts.

3. **Campaign Completed** When all submissions are complete.

4. **Link Clicked** When a target clicks the phishing link — probably the event you will use most.

5. **Credentials Submitted** When the target form submits fake information — the most critical alert.

6. **Aktif toggle** Use this to temporarily disable the webhook; disabling it instead of deleting is safer.

7. **Save Webhook** Saves the configuration. From now on, the selected events start being sent to your webhook URL.

## Payload structure

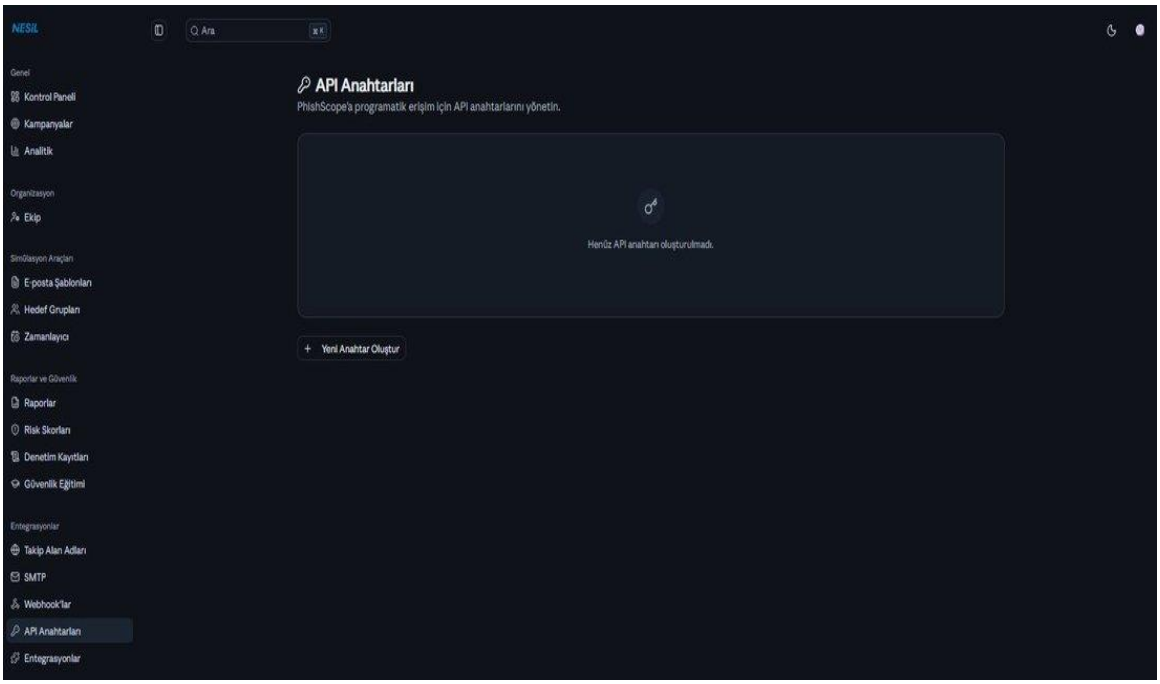
Each webhook call sends a POST body as JSON containing the event type, campaign information, target information, and a timestamp. If your receiving server does not return a 2xx HTTP response, Nesil will retry.

> **Which systems should I connect?**
>
> SIEM (Splunk, Elasticsearch) — For logging all events.
>
> Chat (Slack, Teams) — For pulling "Link Clicked" notifications in real time.
>
> Ticketing (Jira, ServiceNow) — The "Credentials Submitted" event should automatically open a ticket.

> Your own automation (Zapier, n8n, custom backend) — Can connect to any flow you want.

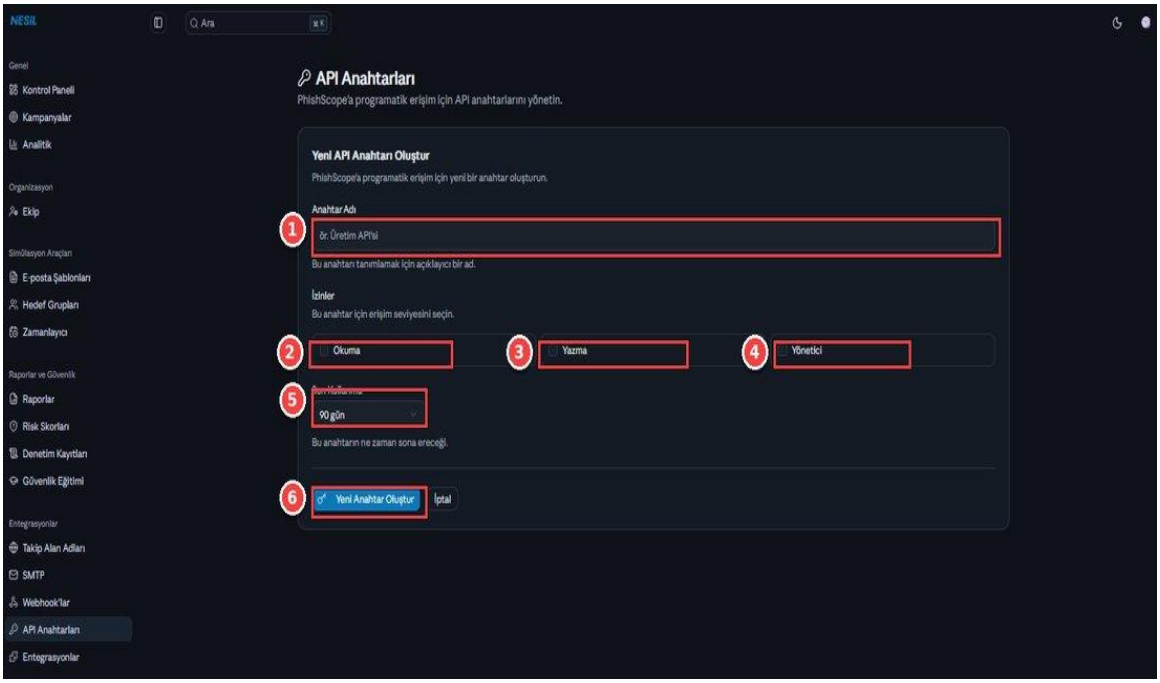
# 26. API Keys

API keys are used for programmatic access to all of Nesil's capabilities. Your own IT team can write an automation, set up an integration with an existing tool (e.g., ServiceNow, Jira), or trigger campaigns from CI/CD pipelines.




*Empty API Keys screen.*

## Creating a new key



1 **Key Name** The internal name of the key — helps you remember where it is used. E.g.: "Production API", "Jenkins Test Pipeline".

2 **Okuma izni** Access to read-only endpoints such as campaign lists and reports.

3 **Yazma izni** Write operations such as creating campaigns and adding targets.

4 **Admin permission** Access to critical endpoints such as settings, team, and billing. Only grant if truly necessary.

5 **Expiration** The period after which the key automatically becomes invalid. Default is 90 days. Avoid long durations for security.

6 **Generate New Key** The key is generated and shown to you once. Do not forget to note it down — you cannot see it again.

**Storing the key is your responsibility**

The API key is shown once after creation and then only the first few characters are visible. If you lose it, you will have to reset it. Do not share it in a Git repo, Slack message, or email; use a secret manager (HashiCorp Vault, AWS Secrets Manager, 1Password).

Create a separate key for each use case — that way if one leaks, you can quickly revoke it.

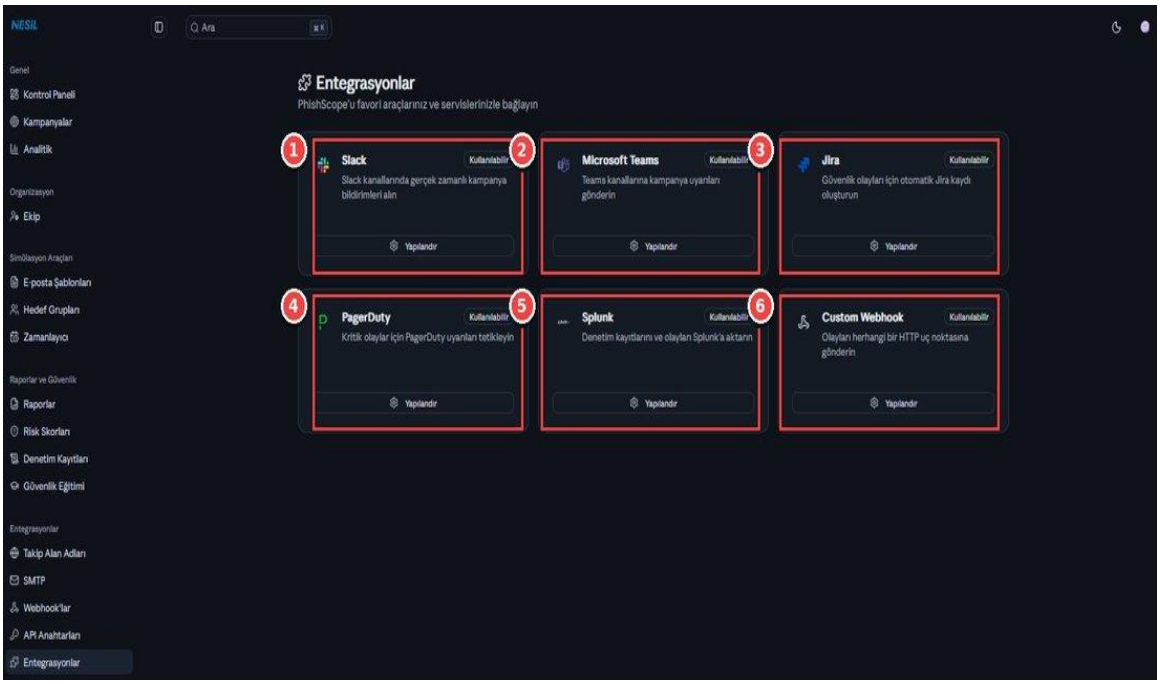
**Anahtar iptali**

If there is a suspicion of a leak, immediately delete the key from the list. Create a new key and update your integration.

If you want to receive advance warning for keys approaching their expiration date, you can enable the relevant option from the "Settings > Notifications" menu.

# 27. Integrations

Webhooks are good for sending data specifically to your own endpoint; but use the Integrations menu to set up one-click integrations with popular tools (like Slack, Microsoft Teams, Jira). This menu lists ready-made connectors.




## Ready-made integrations

1 **Slack** Real-time campaign notifications to your channels. Instant ping to the security channel when a "credential submitted" event occurs.

2 **Microsoft Teams** Campaign alerts to Teams channels. Ideal if your IT teams use Teams as their primary communication channel.

3 **Jira** Automatic Jira record for security events. Opening a separate ticket for each user who took the bait starts the follow-up process automatically.

4 **PagerDuty** PagerDuty alerts for critical events. For waking up the on-call team in cases of large-scale click spikes.

5 **Splunk** Transferring audit logs and events to Splunk. For SIEM-based compliance reporting.

6 **Custom Webhook** Sends events to any HTTP endpoint. If none of the ready-made connectors above fits the need, you can connect to your own system from here.

### Where should I start?

Slack or Teams integration is ideal as the first step for small organizations; it allows you to quickly share catch moments with your team.

In large organizations, Splunk + Jira combination is set up first: Splunk logs every event, Jira opens a tracking record for each event.

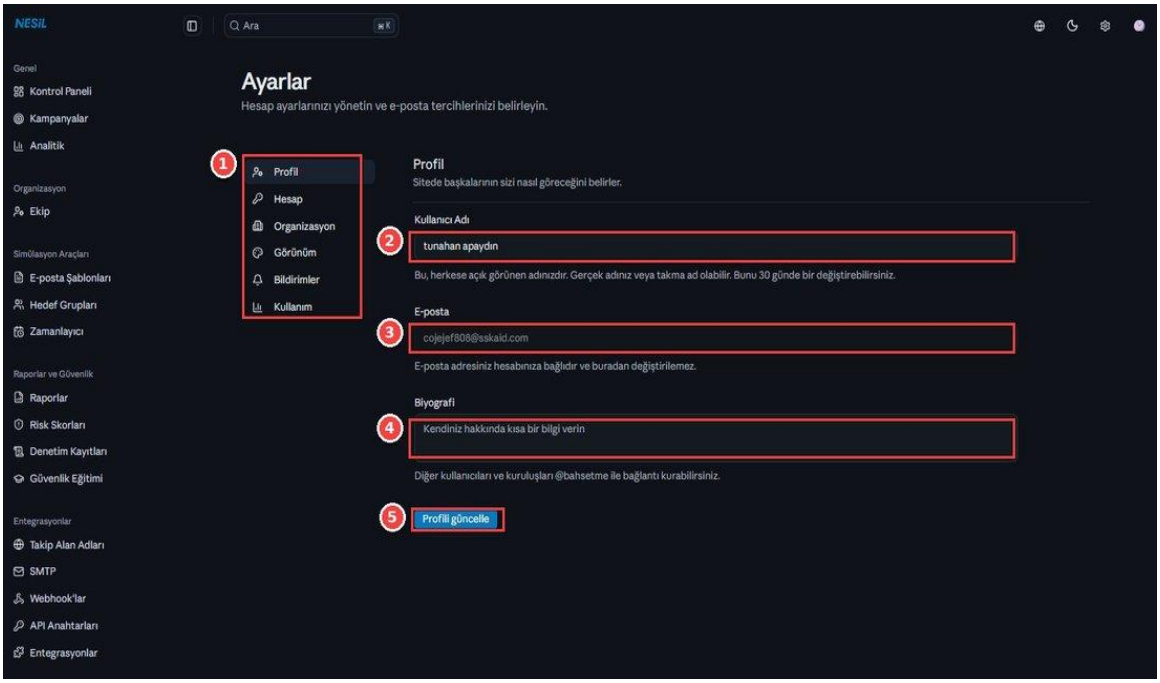
### Each integration comes with an "Available" badge

Your current plan (Enterprise) supports all integrations. Some may not be available on lower plans; you can check your plan information from the Settings > Usage page.

# 28. Settings

The Settings menu that opens when you click the gear icon in the top right brings together account-level and organization-level preferences in one place. There are six tabs: Profile, Account, Organization, Appearance, Notifications, and Usage.

## 28.1 Profil




**1** **Tab menu** Switch between six settings tabs.

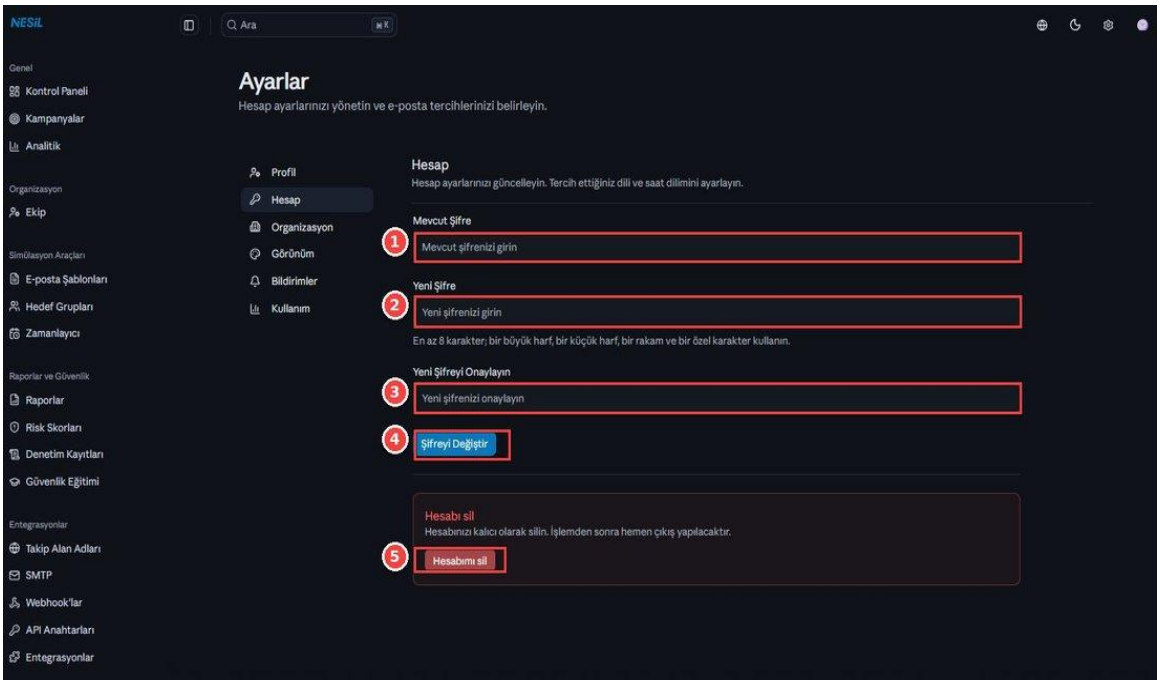
**2** **Username** Determines how others will see you on the site. Can be changed once every 30 days.

**3** **E-posta** The email address linked to your account. Cannot be changed from this field; you need to contact the support team.

**4** **Biyografi** Short description about yourself. The @mention function is used in this field.

**5** **Update Profile** Save your changes.

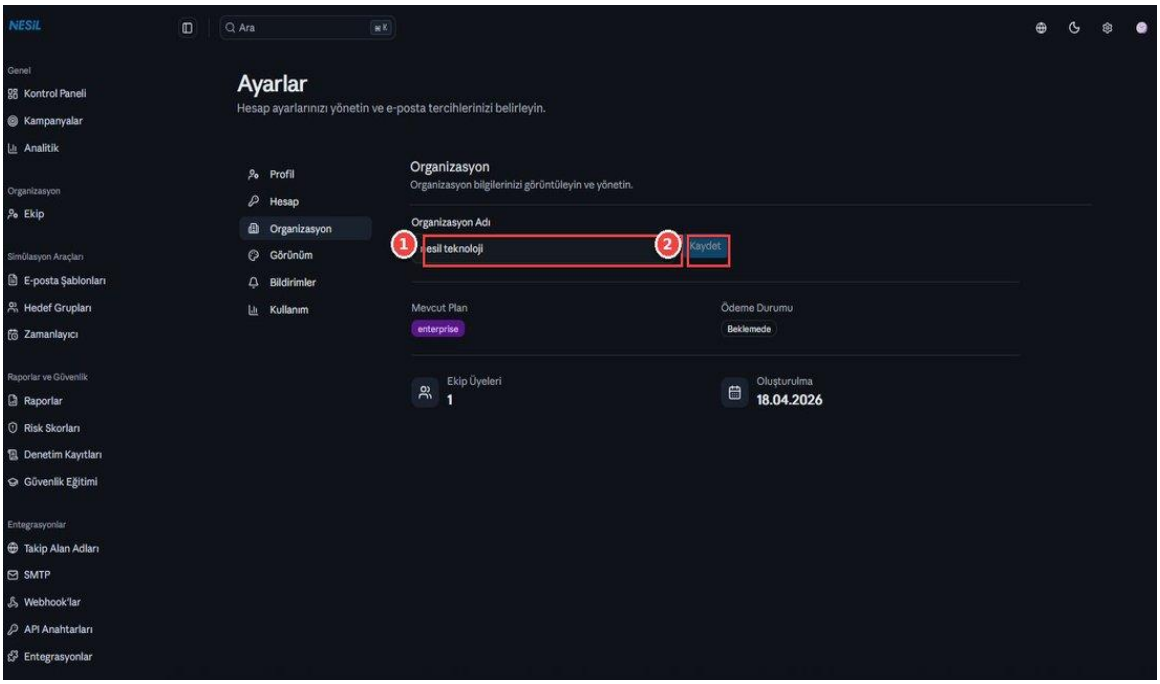
## 28.2 Hesap




| | |
|---|---|
| 1 | **Current Password** Enter your current password for security. |
| 2 | **New Password** Must be at least 8 characters and include uppercase letters, lowercase letters, numbers, and special characters. |
| 3 | **Confirm** Re-enter your new password exactly. |
| 4 | **Change Password** The password is updated; your session is not interrupted. |
| 5 | **Delete My Account** Permanent account deletion. Warning: cannot be undone, all your campaigns and data will be deleted. |

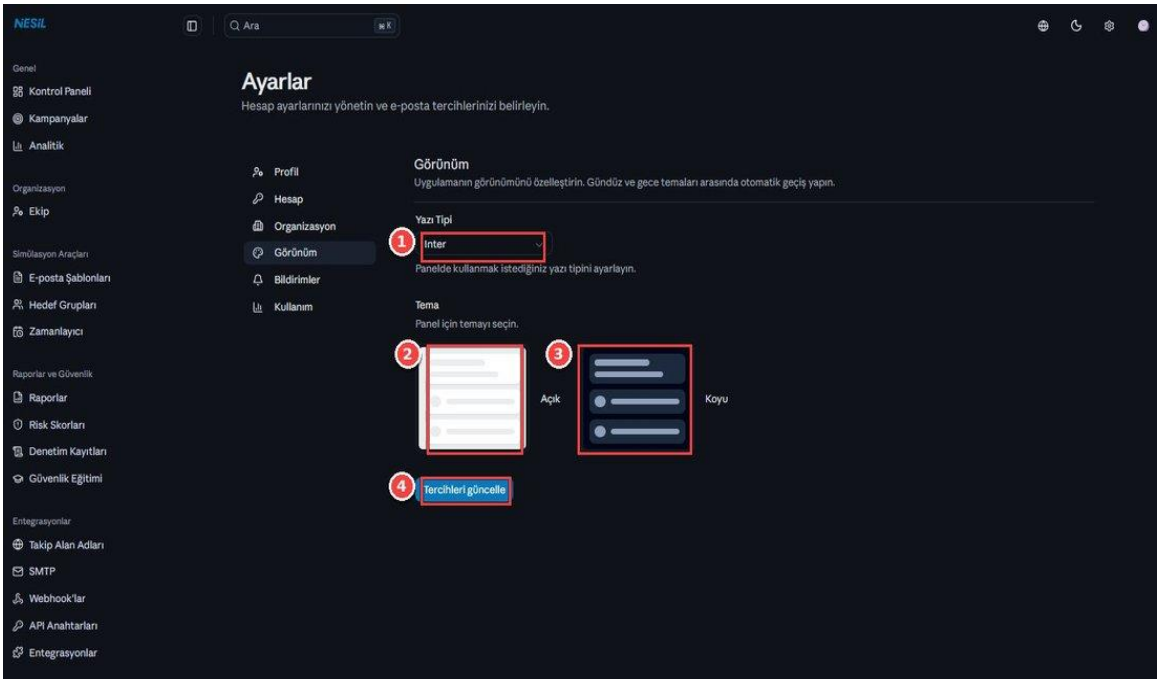
> **Account deletion is permanent**
>
> This action cannot be undone. Campaigns, templates, target groups, reports, audit logs — all are deleted.
>
> If you are simply leaving, it is a safer approach to assign another member with Administrator role and have your own account made inactive.

## 28.3 Organizasyon



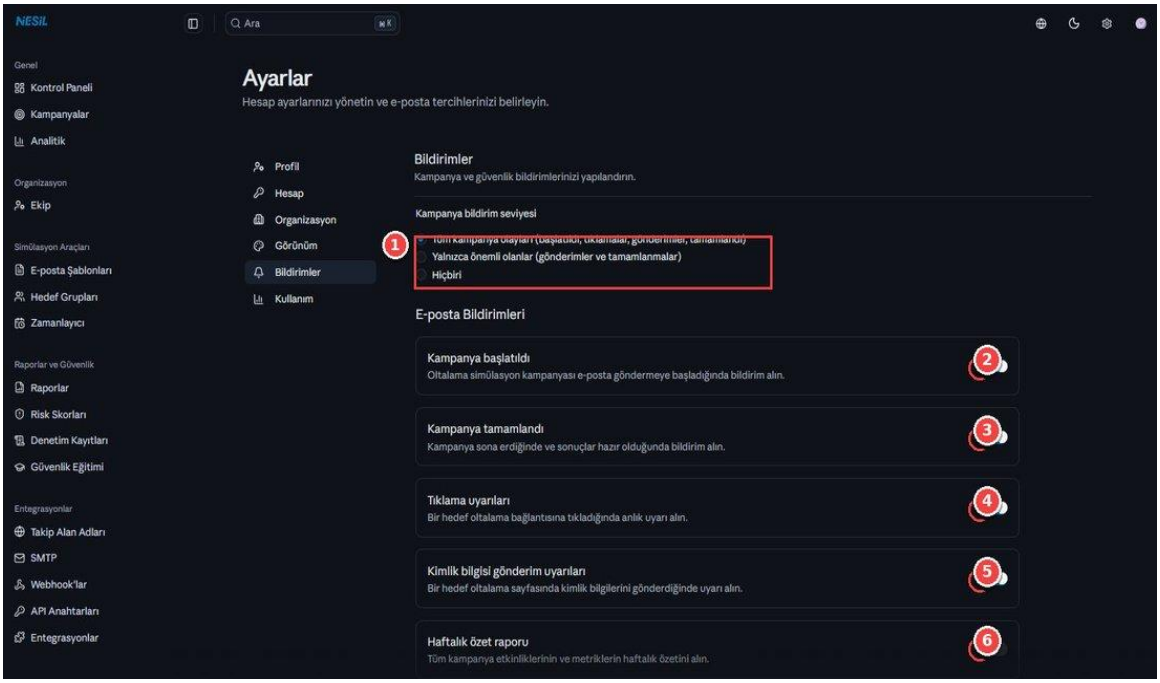

| | |
|---|---|
| 1 | **Organization Name** You can edit the organization name from here. |
| 2 | **Kaydet** Confirms the change. |
| 3 | **Mevcut Plan** The subscription plan you are currently on. |
| 4 | **Payment Status** Billing status: Paid, Pending, Failed, etc. |
| 5 | **Team Members** Total active member count. |
| 6 | **Creation date** The creation date of the organization. |

## 28.4 Appearance



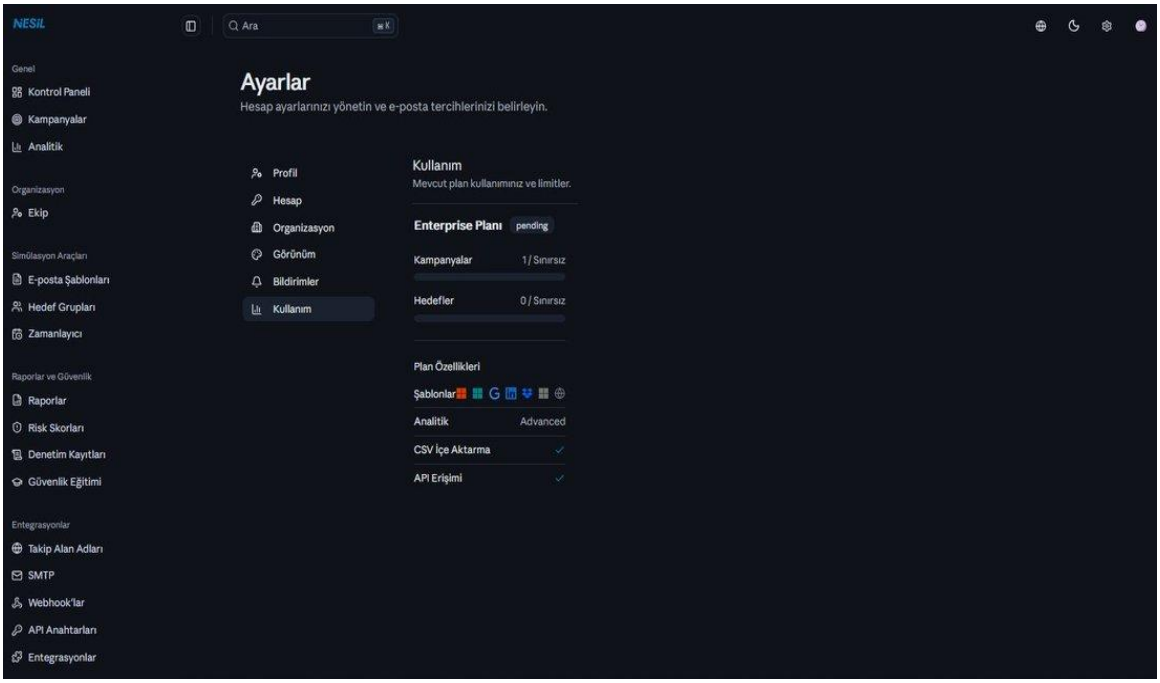

| | |
|---|---|
| 1 | **Font** Select the font to be used in the dashboard (default Inter). |
| 2 | **Light theme** White background, ideal for bright environments. |
| 3 | **Koyu tema** Black background, ideal for nighttime use and the theme seen in all our screenshots. |
| 4 | **Update Preferences** Saves your selections. |

## 28.5 Bildirimler




| | |
|---|---|
| 1 | **Campaign notification level** All events / Important only / None — determines how frequently you want to receive emails. |
| 2 | **Campaign launched** Notifies you when a campaign starts sending. |
| 3 | **Campaign completed** Notifies you when all submissions are finished. |
| 4 | **Click alerts** Instant alert when a target clicks. |
| 5 | **Credential submission alerts** When the target form submits fake information — the most important alert. |
| 6 | **Weekly summary report** Receive a summary of the previous week via email every Monday. |

## 28.6 Usage




The usage limits and features of your current plan are summarized here:

- Campaigns — How many campaigns you have created and the percentage of your limit.
- Targets — Total number of targets.
- Plan Features — List of special features you have (number of templates, advanced analytics, CSV export, API access).

> **Do not leave notifications as they are**
>
> If you leave click alerts on, especially in large campaigns, your inbox will fill up. Our recommendation: select the "Important only" option and track critical events via webhook/Slack integration.

# 29. Quick Reference and Frequently Asked Questions

## Quick start: your first campaign in 15 minutes

After getting to know the platform, setting up your first campaign is surprisingly fast. Here are the steps in order:

1. **Create an account** Enter your organization information from the Create Account screen.
2. **Configure SMTP settings** Connect your sending server from the Settings > SMTP menu.
3. **Choose a ready-made template** Click on one from the Email Templates > Office 365 Password Reset gallery.
4. **Create a target group** Target Groups > Create Group → add 3-5 test targets inside.
5. **Create a campaign** Campaigns > New Campaign → write the name, select the template.
6. **Add targets** In the campaign detail, Add Targets > Groups tab → select your group.
7. **Launch the campaign** Press the "Launch Campaign" button. The system starts sending.

## Most frequently asked questions

### My click rate is very high — is that normal?

Rates of 15-25% in the first drills are perfectly normal. In fact, it is said that the average security awareness of an organization worldwide is around 30%. It is possible to bring these rates below 5% within 3-6 months with repeated training and simulations.

### My targets are not receiving emails

There are several possible reasons: SMTP configuration is incorrect; DKIM/SPF records are missing; the spam filter in the recipient's inbox blocked it. First check the server connection via Settings > SMTP > Test Connection. Then verify delivery status by sending a test campaign to your own email.

### I want to remove a target from the campaign

Go to the Targets tab on the campaign detail page. Click the red delete icon on the right of the relevant row. Even if the campaign has been launched, no more submissions will be made to this target — but an email already sent cannot be recalled.

### Where is the API documentation?

After API keys are generated, there is a detailed documentation link next to each key. Endpoints are REST-based and can be easily consumed in most modern programming languages.

### Do I need to delete old campaigns?

If you are not approaching your plan limit, there is no need to delete them. Old campaigns are valuable for reporting and comparison — comparisons like "my click rate was 20% 6 months ago, now it's 8%" are only possible when data is preserved.

### How do I manage multiple organizations?

Nesil assigns one organization per email address. If you want to manage multiple organizations, you can either open different organizations with different email addresses, or consider the MSP plan — it supports multiple client organizations under a single account.

## Keyboard shortcuts

- ⌘K or Ctrl+K — Focus the search box
- Esc — Close the open modal
- G then D — Go to Dashboard (navigation shortcut in the menu)

## Support and contact

When you encounter any technical issue, the first step is to find the event in the Audit Logs and report it to support with the timestamp. This allows the support team to quickly trace the issue.

- Main site: nesil.ai
- Support: can be submitted via the platform interface (top right > Help > Support Request)

*This guide is a comprehensive reference prepared for you to use the platform effectively. It is updated with new versions; we always keep the most up-to-date version accessible from within the platform.*

***For a secure and aware organization — good work.***