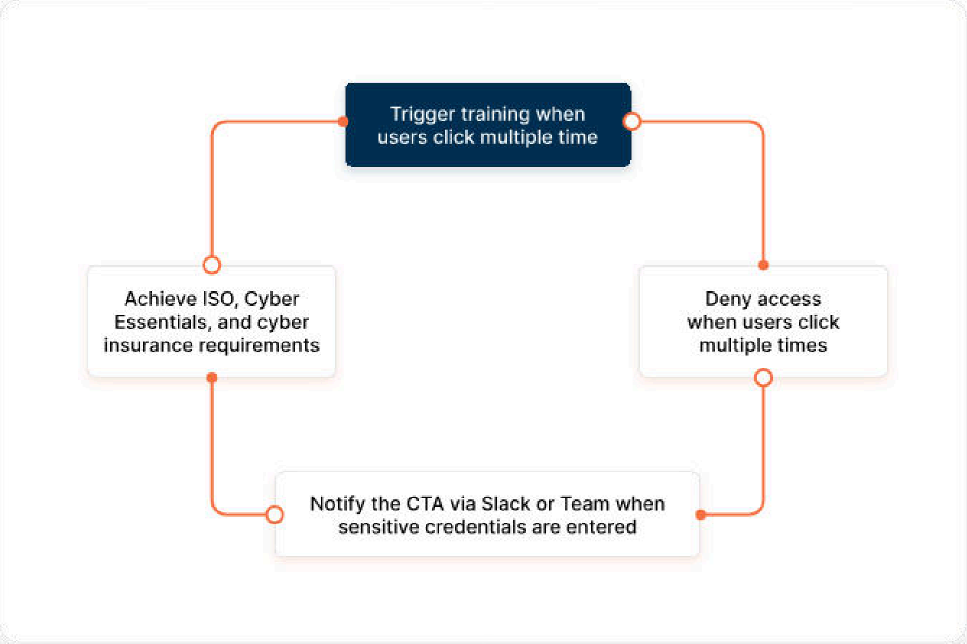
PHISHING
T@CKLE

StarPhish™

StarPhish Workflow Automation


Trigger training when users click multiple time
Deny access when users click multiple times
Notify the CTA via Slack or Team when sensitive credentials are entered
Achieve ISO, Cyber Essentials, and cyber insurance requirements

Introducing StarPhish

Our latest innovation in human risk management

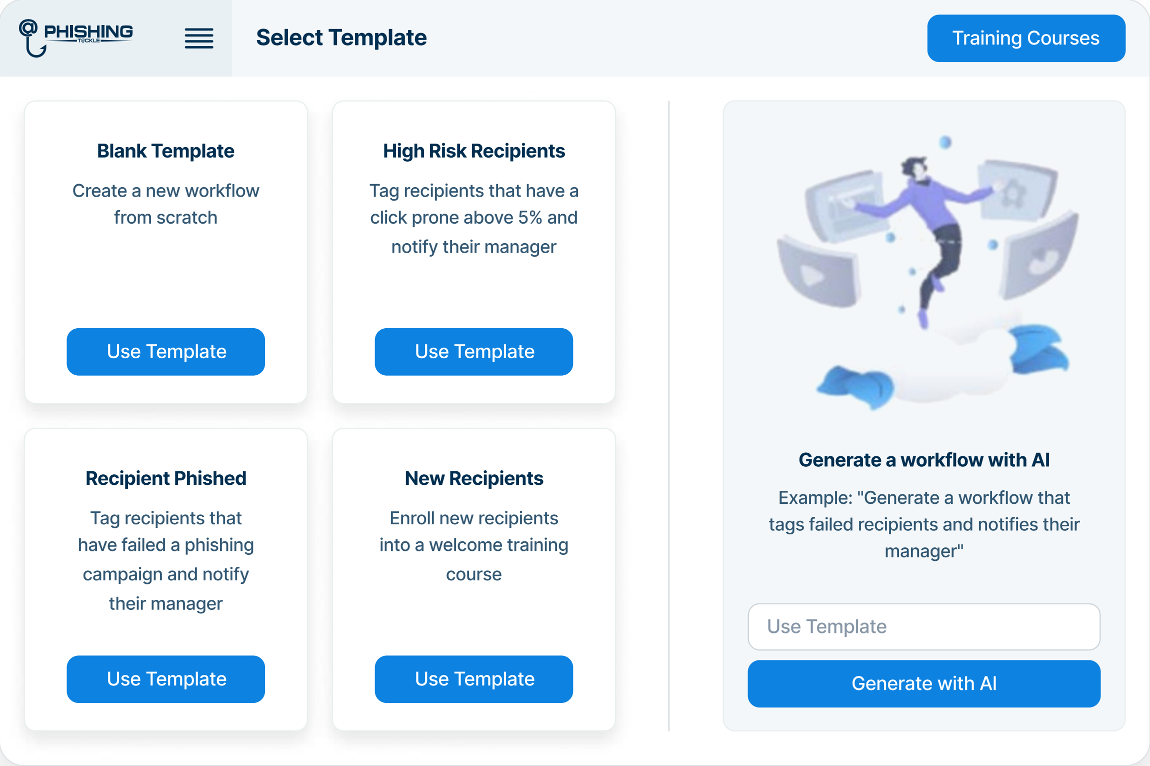
01 Workflow automation offering significant benefits by streamlining and optimising specific, and repetitive, platform processes.

02 AI assisted workflow generation will be able to learn from past data to continuously improve, resulting in more agile, efficient, and scalable operations.

03 Enhanced efficiency by automating tasks that would otherwise require manual intervention, reducing human error and saving time.

PHISHING T@CKLE

AI Assisted or Template Generation



Select Template

Blank Template

Create a new workflow from scratch

High Risk Recipients

Tag recipients that have a click prone above 5% and notify their manager

Recipient Phished

Tag recipients that have failed a phishing campaign and notify their manager

New Recipients

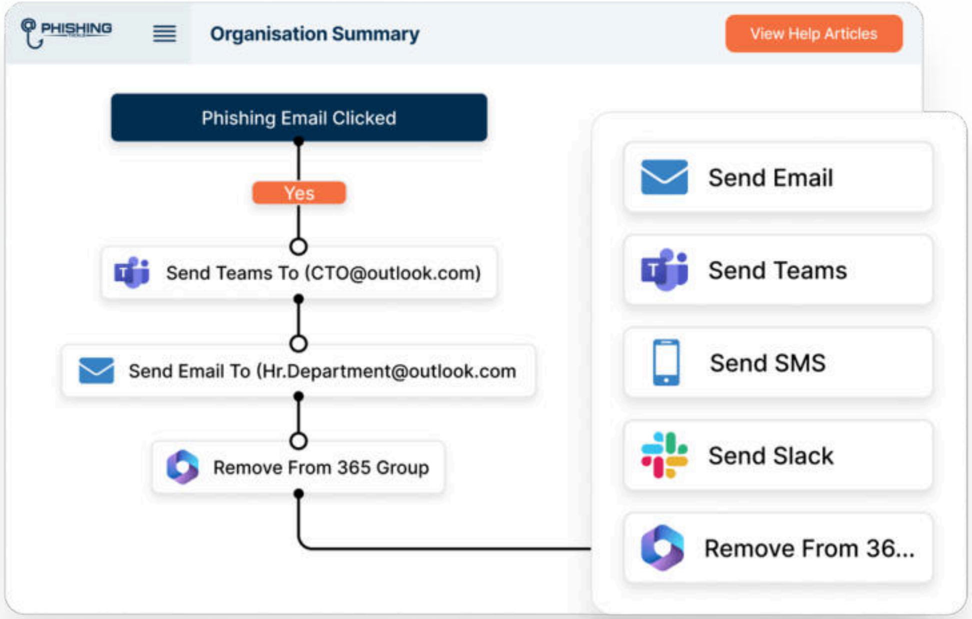
Enroll new recipients into a welcome training course

Generate a workflow with AI

Example: "Generate a workflow that tags failed recipients and notifies their manager"

Workflows are easy to generate using any of our ready-to-use templates, or use AI to assist in the generation of more complex tasks.

Event driven Actions



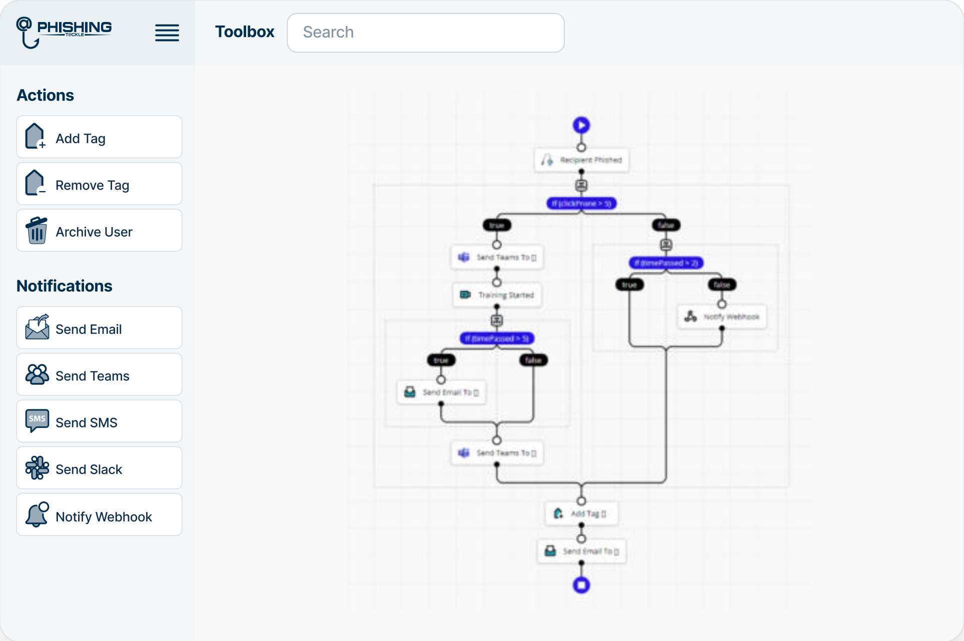
When specific events occur, such as a user clicking on a phishing link or failing a knowledge check, automated actions can be triggered immediately, for example, removing group-access privileges, assigning additional training, sending alerts via Teams, Email, or Slack, or generating reports.

This ensures that corrective measures are taken in real time, reinforcing learning when it's most relevant.

By automating these responses, organisations can ensure that employees receive timely feedback and education, improving their ability to recognise and respond to threats.

This event-action linkage helps maintain a proactive and adaptive security culture.

Drag-and-Drop Workflow Editor



Our drag-and-drop workflow editor makes creating action event relationships intuitive and accessible, even for users without technical expertise.

With a visual interface, users can easily map out the flow of events, such as phishing attempts or security breaches, and link them to corresponding actions, like follow-up training or notifications.

This simplifies the process of building complex workflows, as users can visually connect triggers to automated responses.

The ability to customise workflows through simple drag and-drop functionality enhances flexibility, allowing organisations to tailor training programmes and responses to specific security goals.

This ease of use ensures quicker deployment and continuous refinement of security awareness strategies.

Some of the benefits of StarPhish™

Targeted and Adaptive.

Reactive based on users' interactions with phishing simulations, providing the ability to remove users from high-risk groups and/or customised follow-up training for those who fall for phishing attempts, enhancing learning outcomes.

Real-time Monitoring and Reporting

Automated workflows provide immediate feedback, alerting, and user-based actions. This is especially useful when, for example, a user fails a specific high-risk simulated phishing campaign ensuring timely corrective action, such as blocking the user account and alerting your security team over Slack or Teams.

Time and Resource Efficiency

Automating phishing simulations and follow-up training saves time for educators and administrators by eliminating the need for manual tracking and scheduling, allowing for more focus strategic tasks.

Behavioural Insights and Human Risk Assessment

Track user behaviour over time, providing valuable insights into individual and organisational risk levels, helping tailor future training efforts to high-risk areas.

PHISHING TACKLE