PHISHING TACKLE

What is PhishNet™?

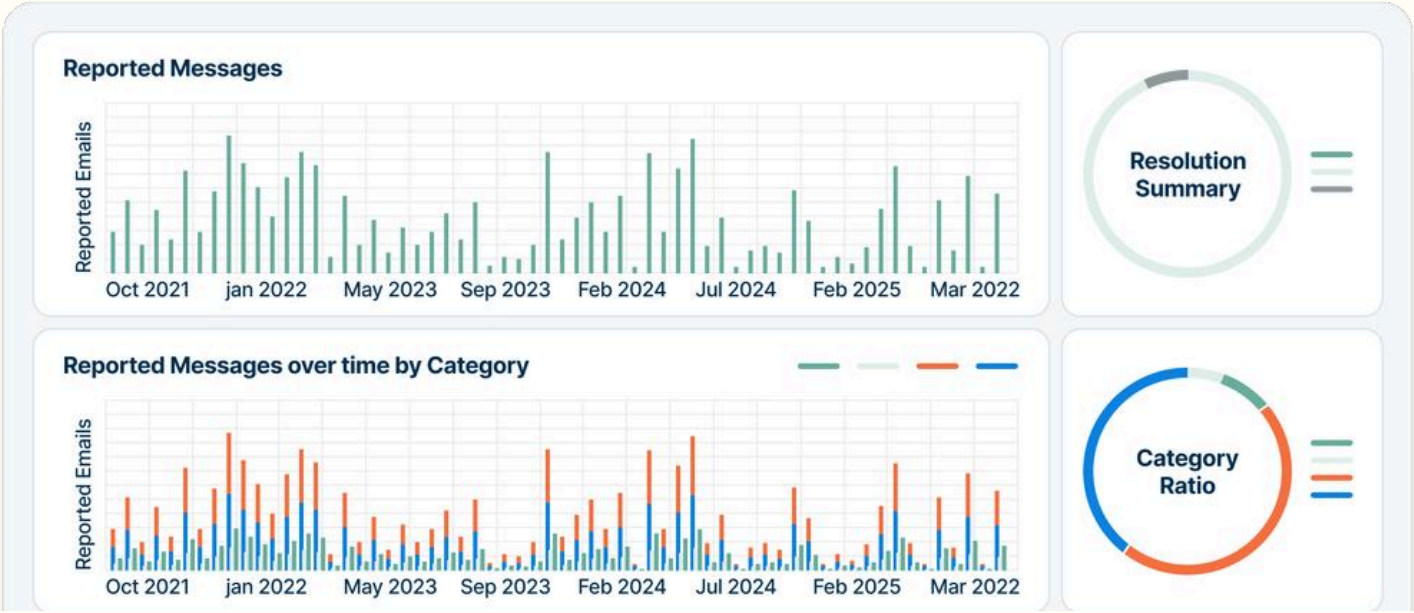
What PhishNet™ can do for your organisation?

How does PhishNet™ tackles a suspicious email?

What is PhishNet™?

PhishNet™ is our Security, Orchestration, Automation, and Response ecosphere (S.O.A.R) within the Phishing Tackle platform. Put simply, this tool provides you with a repository from which you can manage, validate and mitigate potentially malicious emails.

PhishNet™ allows you to prioritise which emails pose a threat to your organisation and allows you to automate an effective response on how to handle them.



How does PhishNet tackle a suspicious email?

A suspicious email arrives
Every day, an average of 9% spam and malicious emails make it through your perimeter protection system and into a user's inbox.

Our Phish Hook® button is used to report it
Your users already use the Phish Hook button to report suspicious emails to your security department. PhishNet™ integrates seamlessly into this process.

PhishNet™ catches the email
Your security team now has direct visibility of the email, including any detail of attachments, domains, links, and more.

YARA rules tackle the email head-on
A simple-to-design algorithmic framework (YARA) is then applied automatically to emails based on their characteristics.

Manual interrogation

Check through your gathered email manually and understand why your users are reporting it. This step helps create new YARA rules and adds further efficiency to this cycle.

Tags automatically categorise the threat

PhishNet™ will tag the email and categories it based on the email's context and messaging.

Check for Malware

Run various malware checks (manually or automatically) on email attachments and URLs to ensure that they are clean.

Automate your response

Automate your responses to all suspicious messages using the simple YARA rule set.

Catch & Release

Phishing Tackle's "catch & release" feature allows your PhishNet™ workflow to automatically convert a malicious email into a reusable simulated phishing template.

This strips all malicious links and attachments and adds them to your template library ready for use in a simulated phishing campaign.

Use as a tool or dispose of it entirely

The email will either be released back to your users or be securely deleted. This is determined by your YARA rules or you manually overriding the decision.

What PhishNet™ can do for your organisation?

S.O.A.R

PhishNet™ is your gateway to Security, Orchestration, Automation, and Response (S.O.A.R). The ultimate goal of any S.O.A.R implementation is to increase the efficiency and efficacy of your security team by reducing the time spent on mundane and repetitive tasks.

With less time spent on repetition, more time can be spent on learning the real threats that exist to your organisation and how to prevent them.

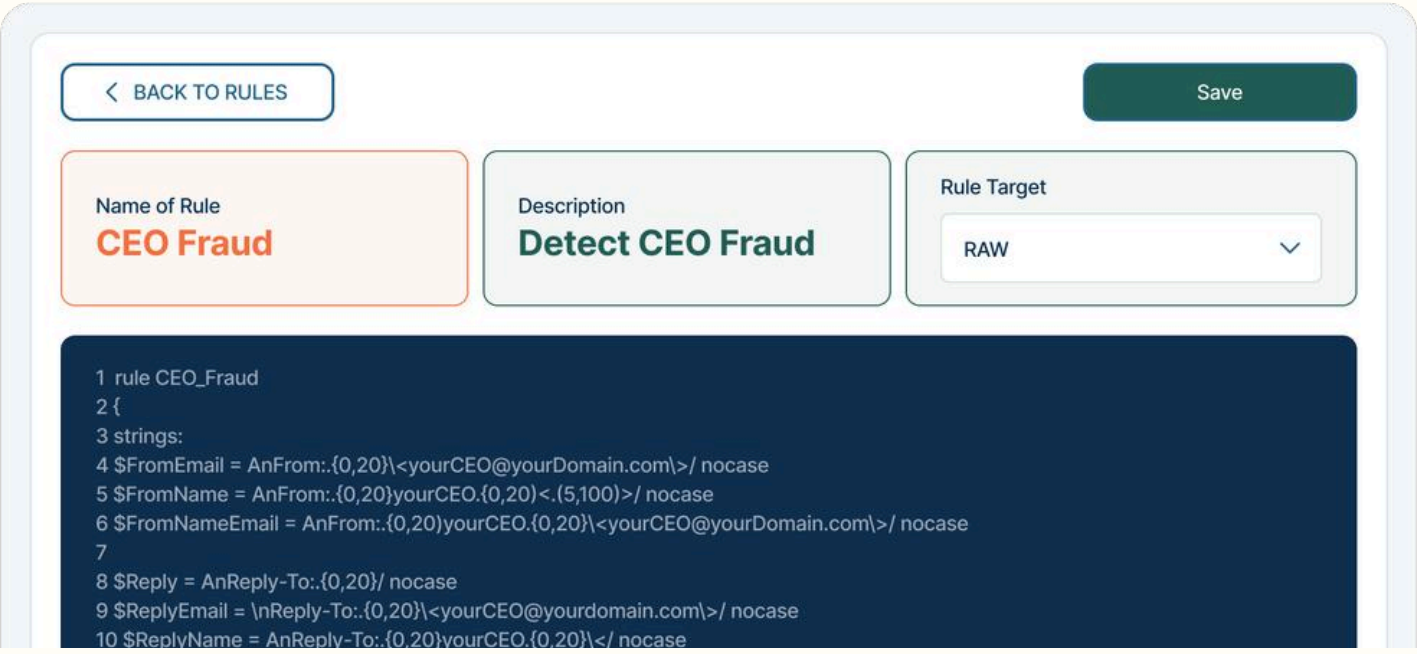
Watch as real threats become real training

PhishNet™'s "Catch & Release™" feature automatically turns your malicious emails into simulated phishing tests for your users, enabling immediate real-world simulations based on actual threats hitting your organisation.

Relax and let the rules work for you

By setting up simple-to-design YARA rules, your security team can create automated paths for emails to take, depending on their characteristics. This allows for an entirely automatic prioritisation process, moving the important emails into individual secure mailboxes for further investigation, deletion, or release back to the user.

With the flick of a switch, these rules can be enabled and disabled according to requirements or called manually from within any email under interrogation.



Remove all doubt with VirusTotal email scanning

Automated scanning of email attachments and URLs can be conducted using our VirusTotal integration. Each item submitted for scanning will be inspected by over 70 anti-virus scanners and URL/domain blacklisting services and appropriate actions can be automatically taken based on this scanning.

Experience total transparency of reported emails

The PhishNet™ dashboard enables an 'X-ray' view into every reported email, allowing full visibility of every included link or attachment. You can also interrogate every level of header information, broken down into easily understandable pieces to further reduce interrogation time.

You can also switch to RAW mode to view every single line of envelope and letter information in raw text.