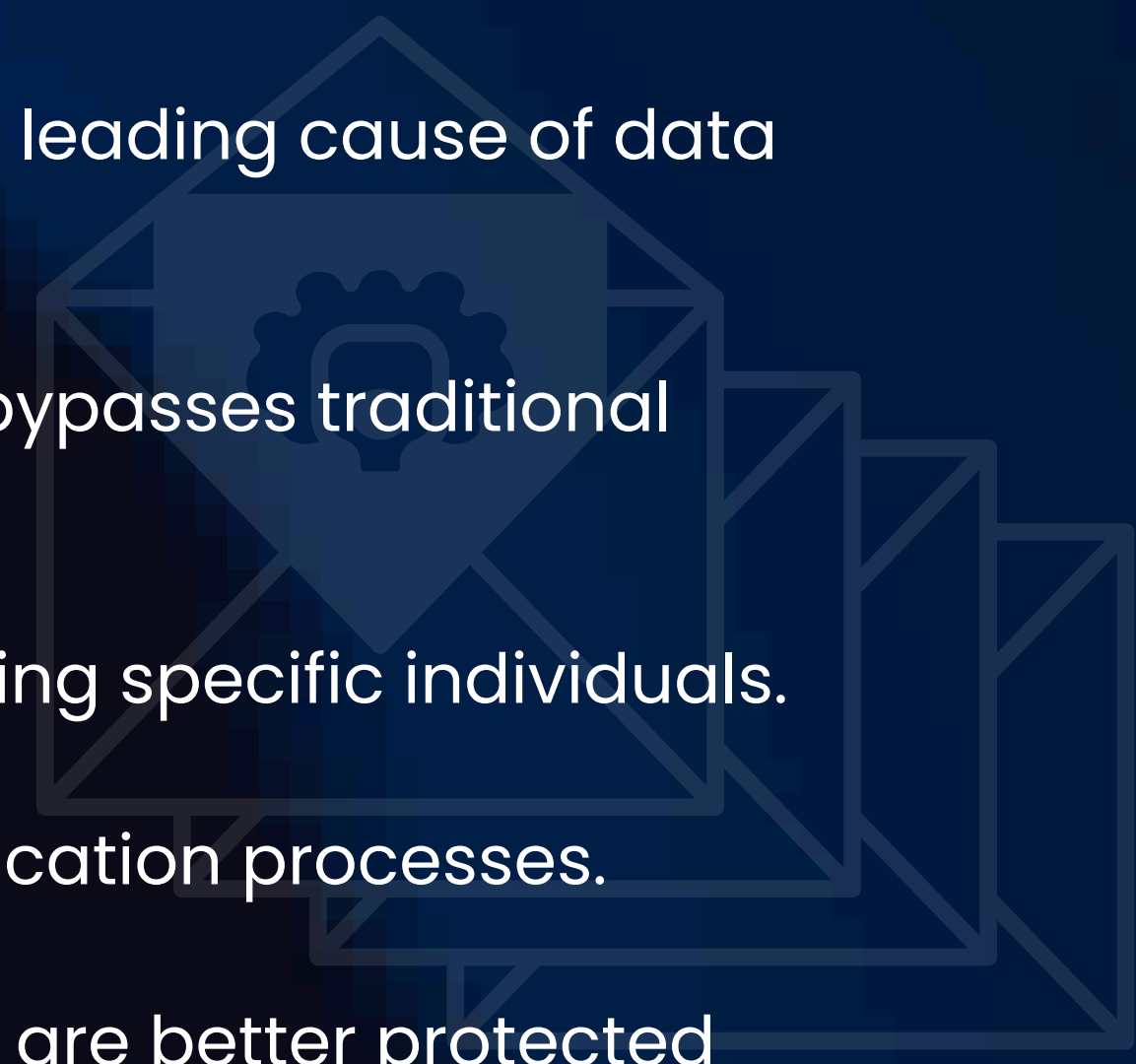




The Risk

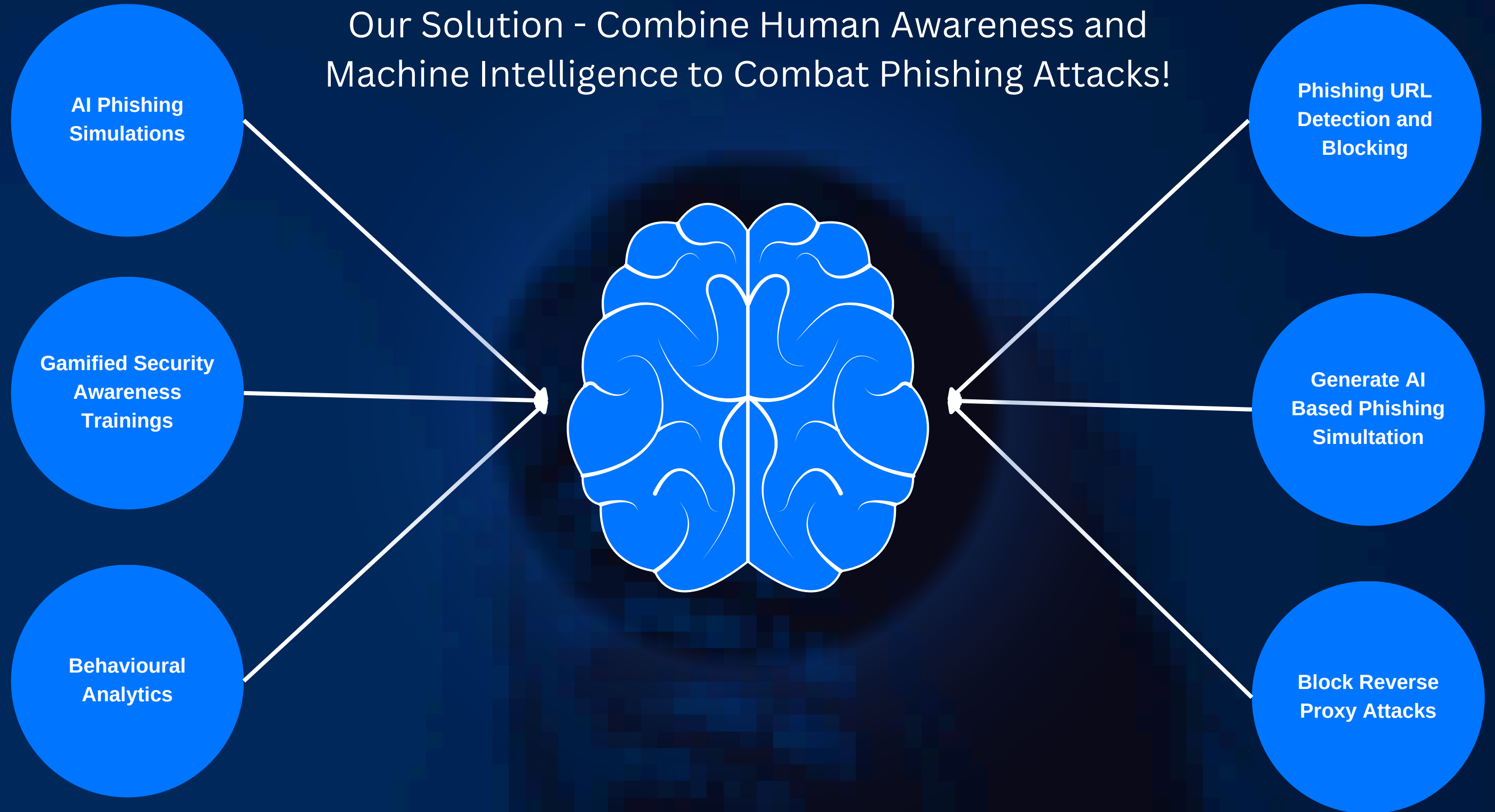
- 90% of breaches are phishing-related, making it the leading cause of data breaches.
- AI-driven attacks like deepfakes and voice cloning bypasses traditional security controls..
- AI personalizes phishing campaigns at scale, targeting specific individuals.
- MFA bypass tactics exploit vulnerabilities in authentication processes.
- Browser-based attacks are on the rise as endpoints are better protected by EDRs.



Your Current Situation

- No phishing prevention platform or traditional solution that does not offer advanced simulations like AI-driven spear phishing, deepfake attacks, and voice cloning.
- Overused generic phishing templates that employees easily recognize.
- No browser-based protection against modern threats (Evilginx, Evil NoVNC, Deepfake video call detection etc.).
- Your team spends hours creating creating custom phishing templates.

Our Solution - Combine Human Awareness and Machine Intelligence to Combat Phishing Attacks!



Awareness Trainings

Browser Based phishing prevention

LetsPhish Overview

AI-driven phishing simulations to train employees.

Real-time awareness training tailored to evolving threats.

Interactive security awareness games to train employees.

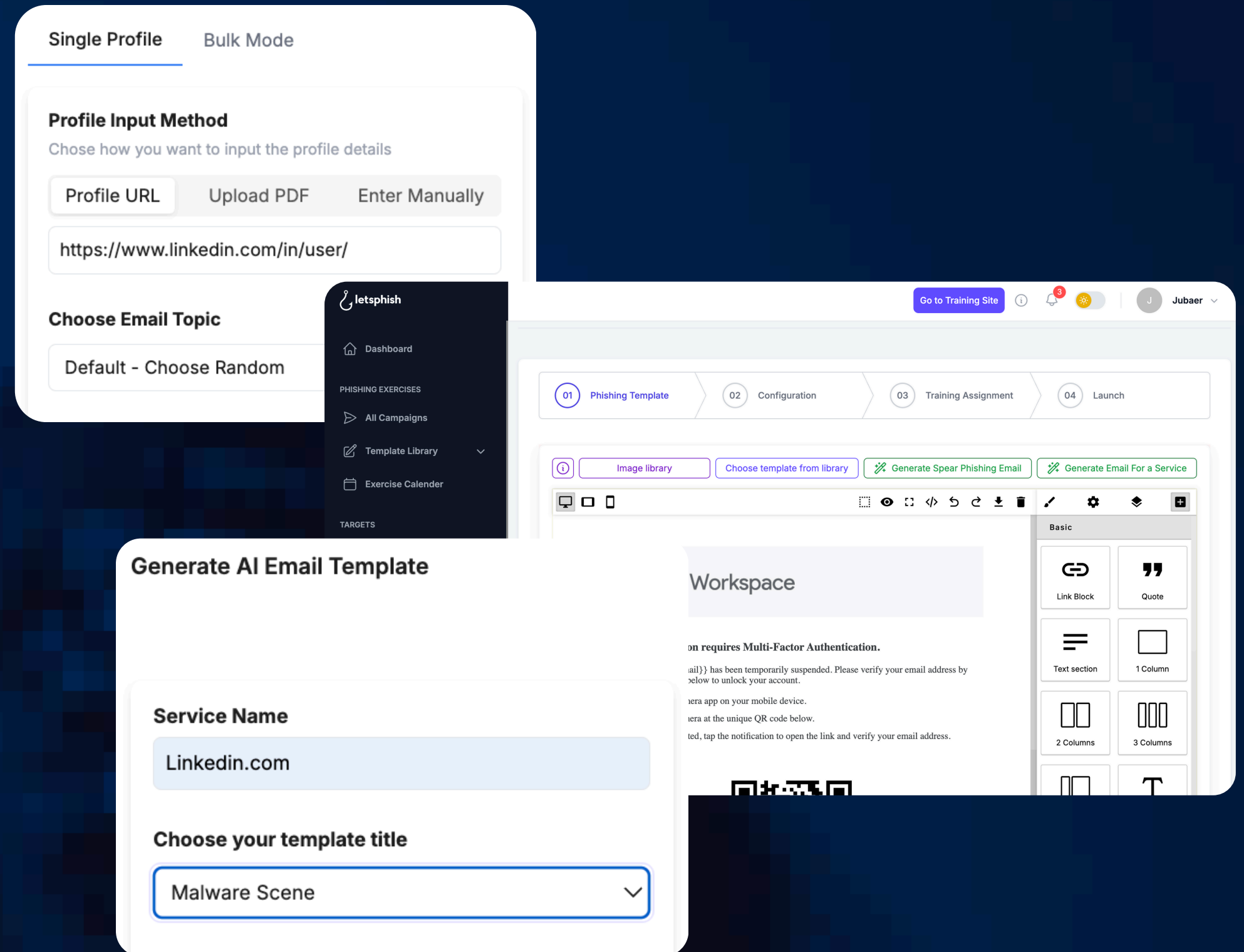
Deepfake & voice cloning simulation training to prevent fraud.

Browser agent protection to prevent credential theft

AI Email Generation

Train employees with AI-generated phishing attempts that mimic real-world attacks.

AI analyzes user behaviours to improve phishing simulations over time.



Vast Email Templates Collections

Access an extensive collection of pre-built phishing email templates tailored to different attack scenarios.

Generate customized phishing email templates instantly based on real-time threat intelligence.

Choose Phishing Template

Search

Search template


Visibility

☐ Private

☐ Public


Service Name

e.g., okta.com



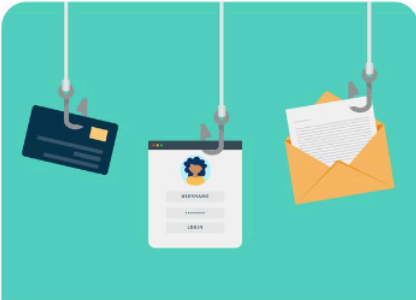
DocuSign Sign Document Email

PreviewSelect



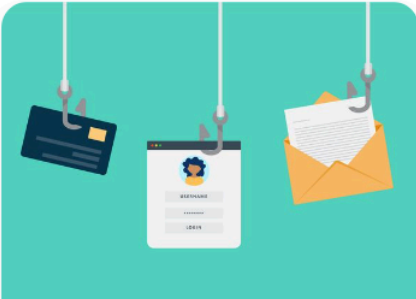
Slack Password Reset Email

PreviewSelect



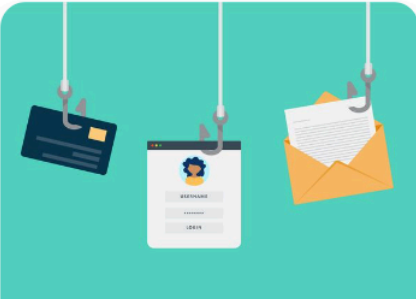
You invited a user to QuickBooks

PreviewSelect



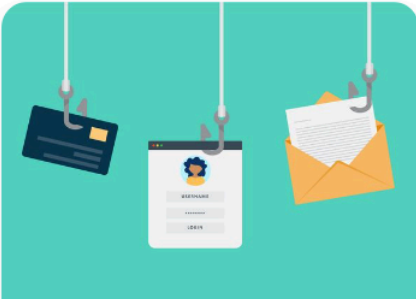
Locked out of account after failed login attempts

PreviewSelect



Pento Password Expiry Email

PreviewSelect



BigCommerce Security Alert

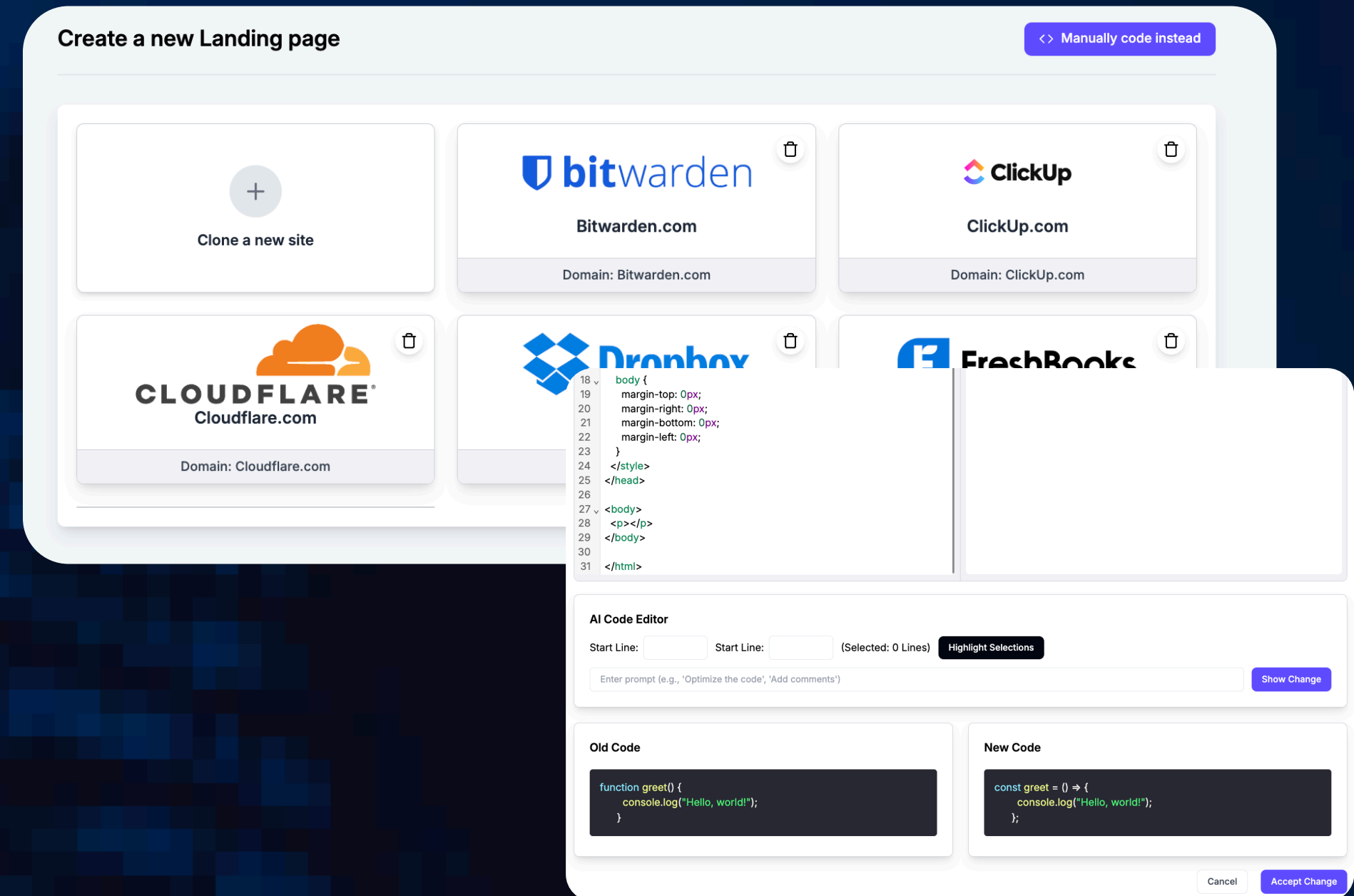
PreviewSelect

Landing Page Cloning

Landing page cloning using a browser add-on for realistic attack simulations.

Browser Add-On for Seamless Cloning: Easily replicate phishing sites with just a few clicks.

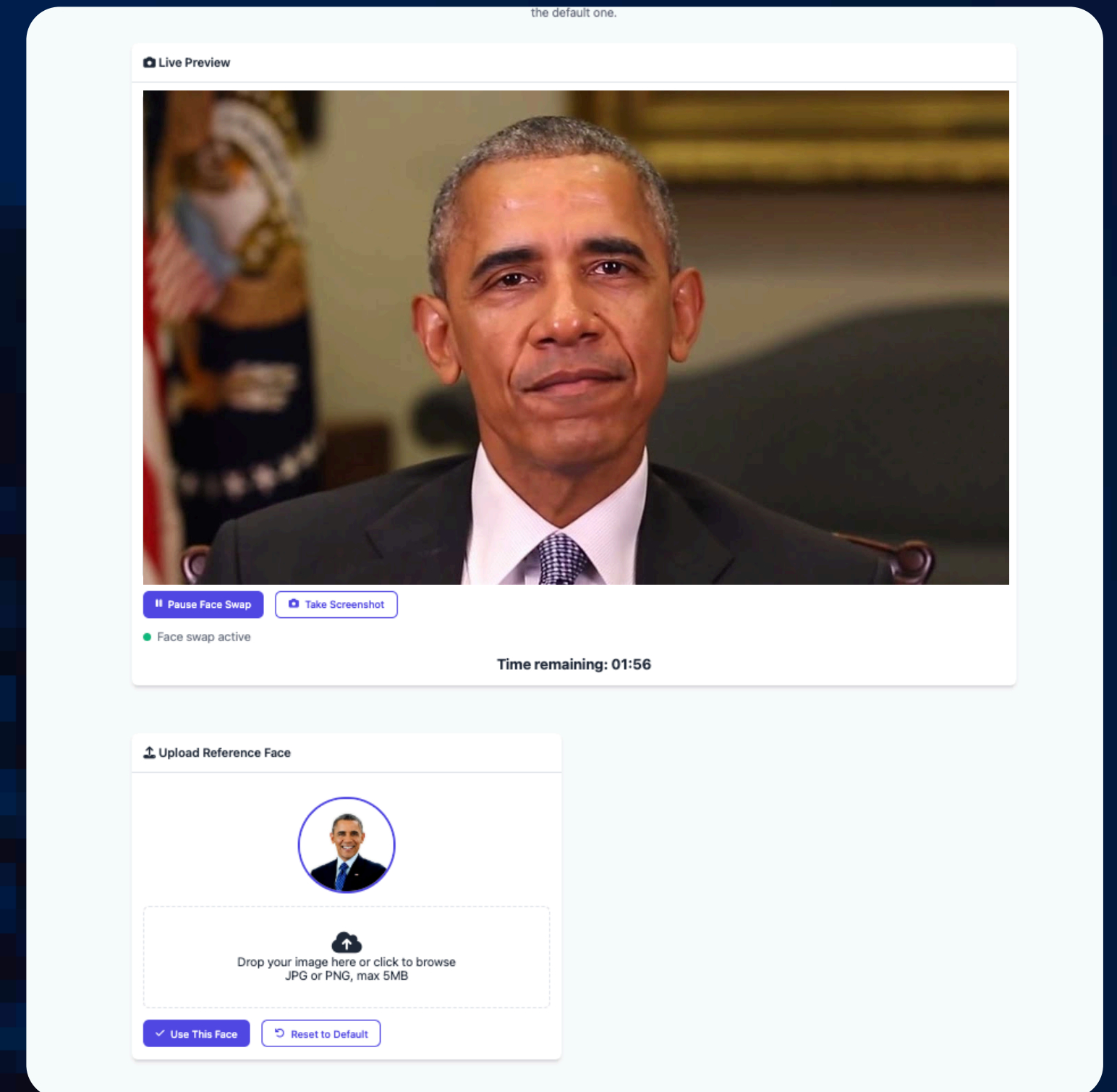
Customizable Templates: Clone targeted login pages, portals, and corporate dashboards for training.



Deepfake and Voice Cloning Simulation

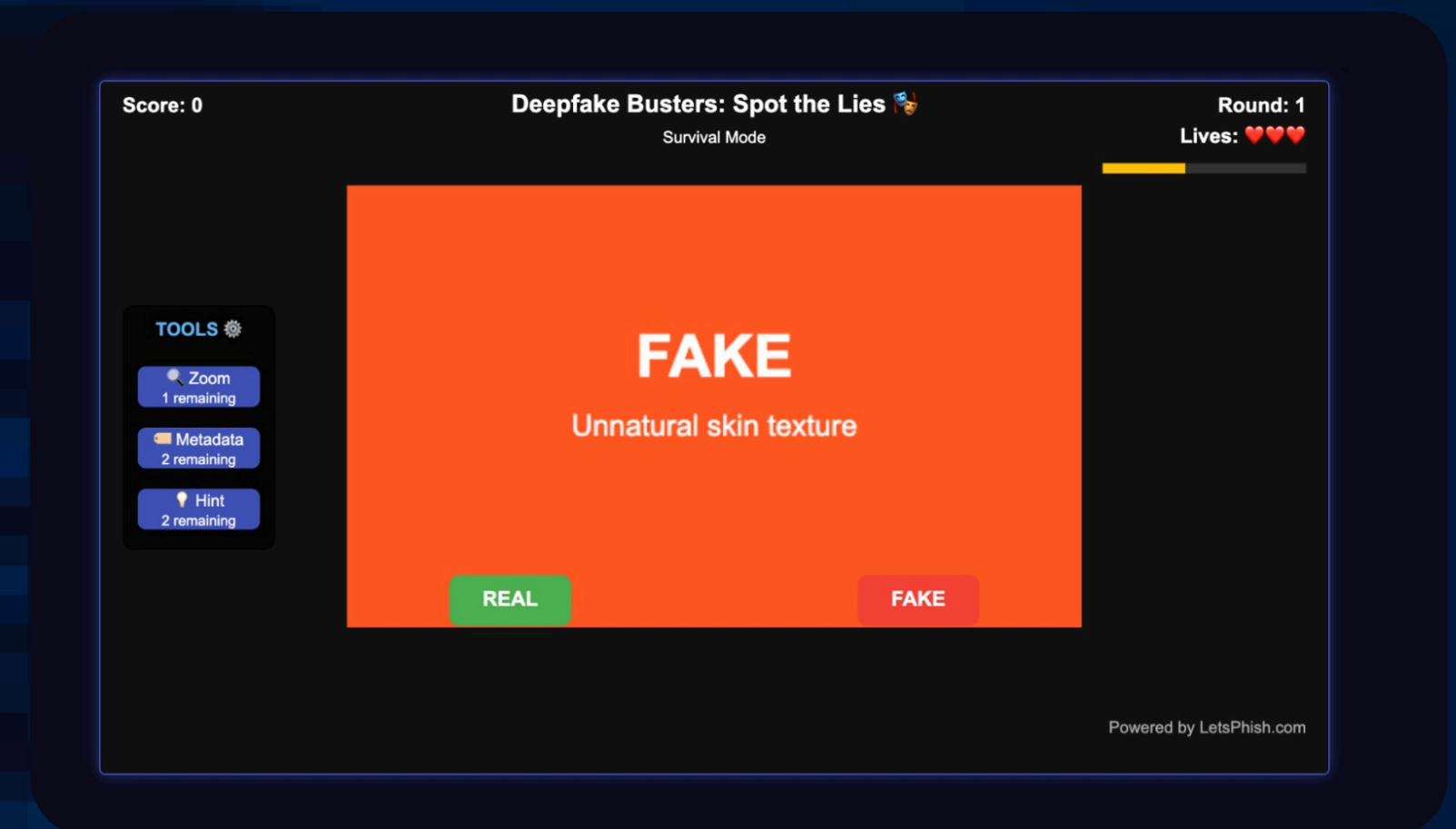
Realistic Deepfake Scenarios: Create AI-generated videos that mimic executives, employees, or trusted authorities to test awareness.

Voice Cloning Attack Simulations: Simulate AI-powered voice fraud and test organizational readiness against CEO fraud and digital impersonation.



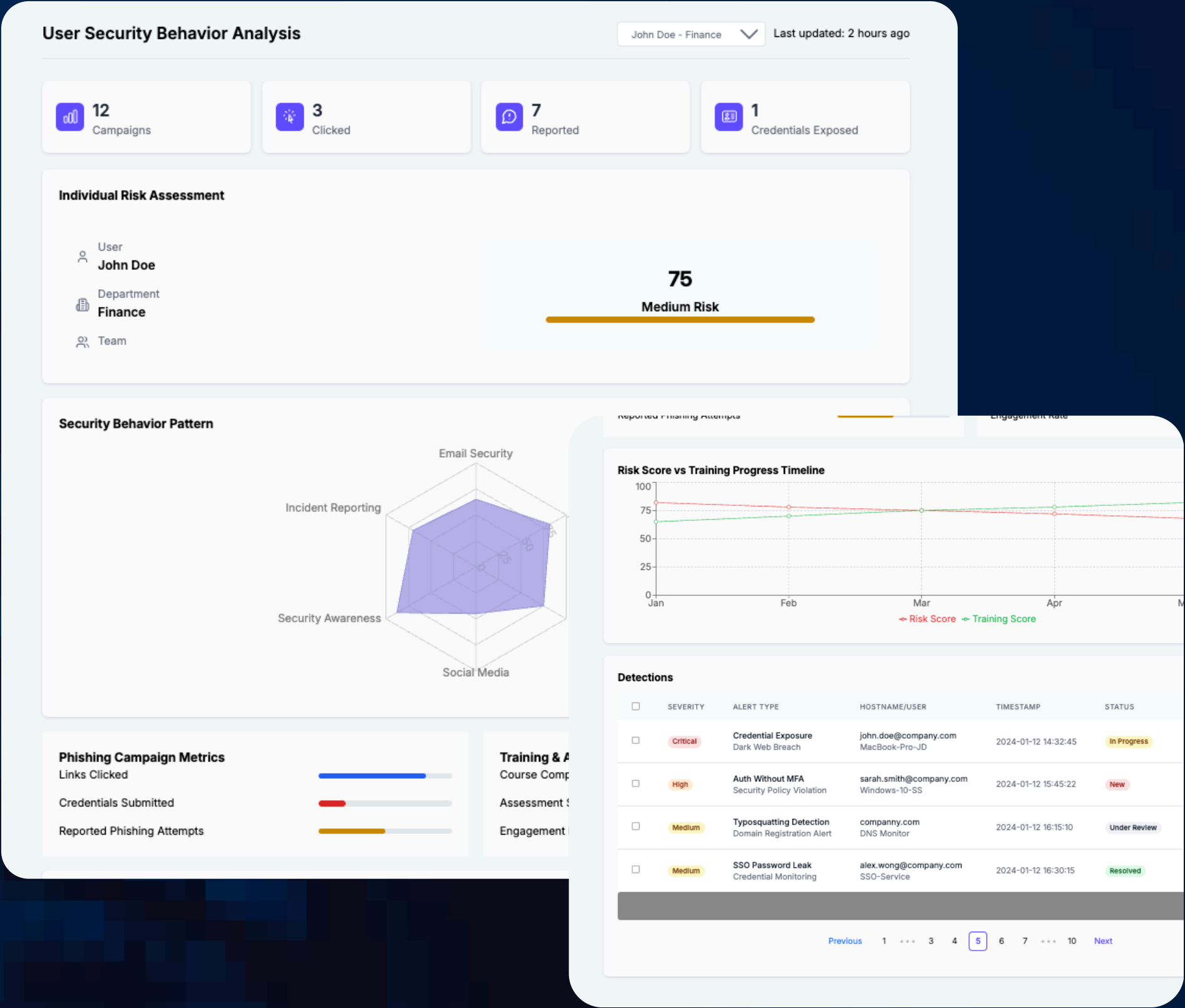
Interactive Security Awareness Games

Interactive games offer a dynamic and engaging way to train employees and security teams in identifying and responding to cyber threats. These gamified scenarios immerse users in real-world-inspired challenges, enabling them to experience both the mindset of an attacker and the strategies of a defender.



User Security Behavior Analysis

The feature tracks the user's adherence to best practices in areas like email security, password hygiene, data handling, and incident reporting. It provides a snapshot of their security behavior, helping identify strengths and weaknesses.



Threat Map

The Threat Map is an all-time view that gives a snapshot of the user's interactions with threats and training progress, helping security teams understand the user's behavior, vulnerabilities, and the effectiveness of ongoing training initiatives.



Training Courses

Our courses offer realistic, simulated phishing emails that mimic common tactics used by cybercriminals. These scenarios are designed to reflect actual phishing campaigns, including various forms such as spear phishing, whaling, and social engineering.

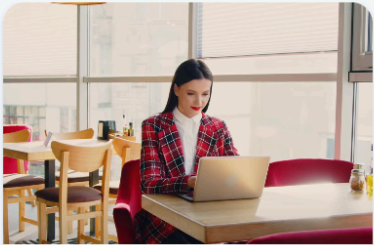
Course Library

Create new course

Search

Search template


Category



Remote Work Security Awareness: Protect Your Data and Stay Safe Online

Details


Assign



Physical Security Awareness: Protect Your Workplace and Personal Space

Details

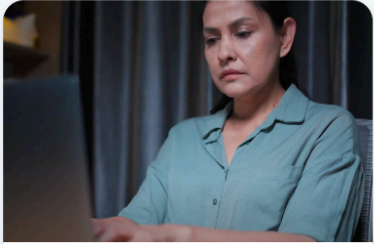
Assign



Internet & Browser Security: Protect Yourself from Online Threats

Details

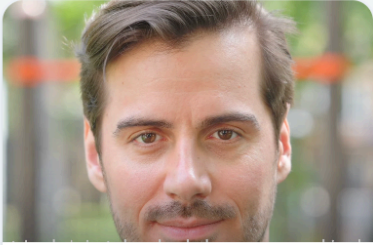
Assign



Phishing Email Awareness

Details


Assign



Mobile Security Awareness: Protect Your Smartphone from Threats

Details

Assign



Password Manager Security: Keep Your Accounts Safe & Secure

Details

Assign

AI Assistant

LetsPhish Assistant is an AI-powered tool that automates phishing campaign creation, scheduling, and targeting. It generates realistic phishing scenarios, tracks performance, and helps improve security awareness with minimal effort, ensuring campaigns stay up-to-date with the latest tactics.

Hi there, **Jubaer**
What can I assist you with today?

Help me create a phishing campaign targeting software developers

Generate an phishing email template for okta.com

Create a target group targetting new joiners

Analyze my campaign results and suggest improvements

Ask whatever you want...



LetsPhish Shield

The letsphish browser agent provides advanced protection against a wide range of phishing and cyber threats. It detects sophisticated attacks such as **Evilginx**, **EvilnoVNC**, and typo-squatting, as well as vulnerabilities like SSO password leaks. Additionally, it identifies deepfake attempts in platforms like Google Meet, ensuring that your users are safeguarded against both traditional and emerging cyber risks in real-time.

Detections

Deploy Browser Agent

10

Critical Alerts

20

Pending Review

24

Resolved Today

11

MTTR (hours)

Search alerts...

All Severities

All Statuses

Export

	SEVERITY	ALERT TYPE	HOSTNAME/USER	TIMESTAMP	STATUS	ACTIONS
<input type="checkbox"/>	Critical	Credential Exposure Dark Web Breach	john.doe@company.com MacBook-Pro-JD	2024-01-12 14:32:45	In Progress	<div>View Details</div> <div>Analyse</div>
<input type="checkbox"/>	High	Auth Without MFA Security Policy Violation	sarah.smith@company.com Windows-10-SS	2024-01-12 15:45:22	New	<div>View Details</div> <div>Analyse</div>
<input type="checkbox"/>	Medium	Typosquatting Detection Domain Registration Alert	company.com DNS Monitor	2024-01-12 16:15:10	Under Review	<div>View Details</div> <div>Analyse</div>
<input type="checkbox"/>	Medium	SSO Password Leak Credential Monitoring	alex.wong@company.com SSO-Service	2024-01-12 16:30:15	Resolved	<div>View Details</div> <div>Analyse</div>

Previous

1

...

3

4

HTTP Request Flow Analysis

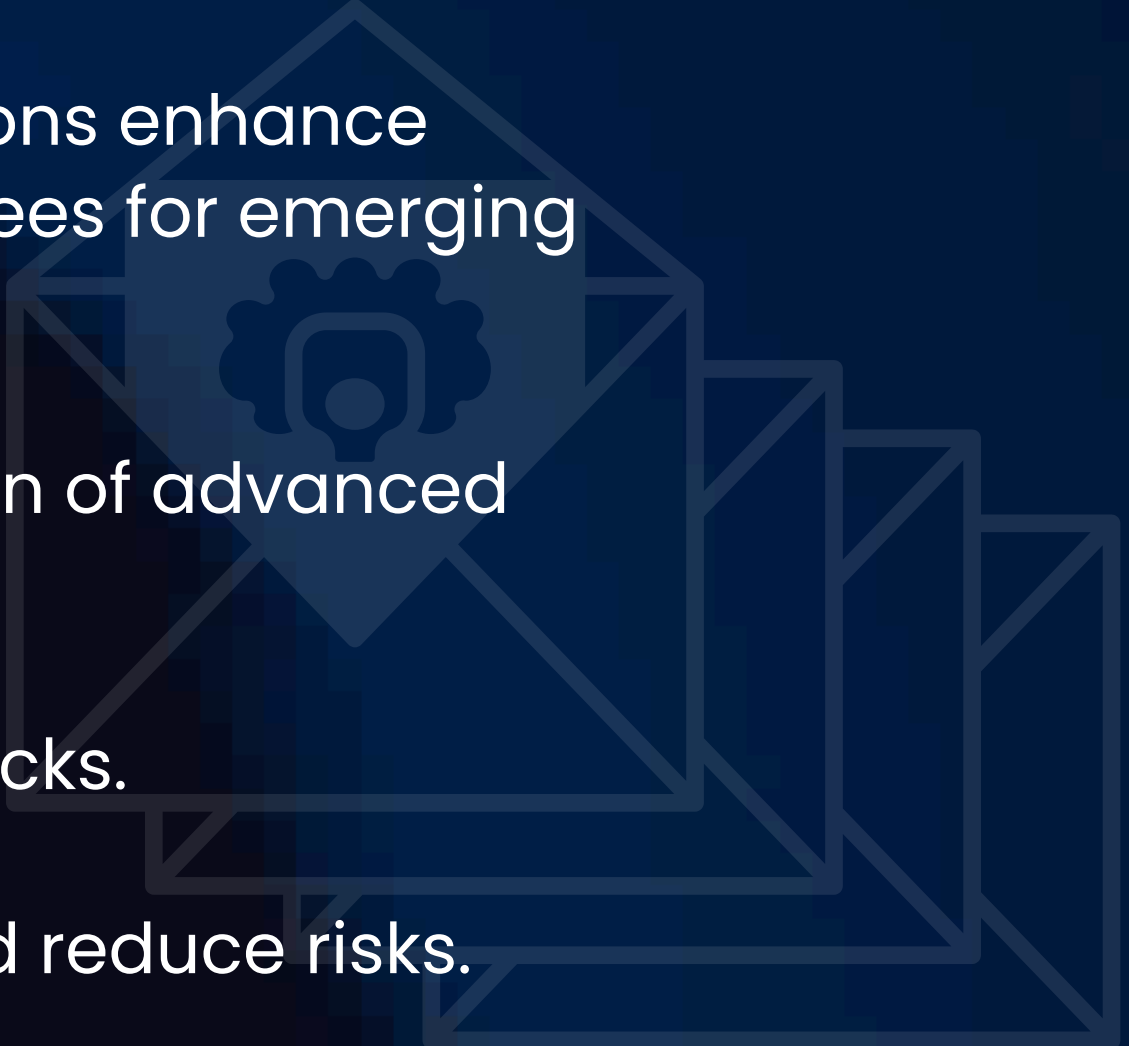
evilforum.com
HTTP Referrer

link clicked

okta-login-portal.com
Typosquatting domain detected

Typosquatting Alert
Similar to Legitimate Domain: okta.com

Expected Outcomes

- **Stronger Employee Awareness** – AI-driven simulations enhance recognition of phishing threats and prepare employees for emerging cyber risks.
 - **Enhanced Threat Detection** – Improved identification of advanced attacks.
 - **Reduced Incidents** – Fewer successful phishing attacks.
 - **Compliance & Risk Reduction** – Meet standards and reduce risks.
 - **Actionable Insights** – Track progress and measure improvements.
- 

Our Backstory

A few years ago, we (the founders) worked at a trading company where disaster struck. An attacker exfiltrated our most sensitive data and demanded a ransom. The entire company was paralyzed, and our reputation was on the line. After investigating, we discovered the breach was caused by something so simple yet devastating—a single employee clicked a link in a phishing email.

It was a wake-up call. Despite all the firewalls and security tools, we overlooked the weakest link: human error. That moment stuck with us and inspired us to build LetsPhish.

Contact Us

We're here to help!

For inquiries, support, or more information about our services:

- Email: info@letsphish.com
- Website: www.letsphish.com

Social Media:

- LinkedIn: [@letsphish-com](https://www.linkedin.com/company/letsphish-com)

Schedule a demo today to see how letsphish can enhance your security awareness training!