

Build a more security-conscious and ethically aligned workforce

Catalyst Phishing is LRN's next-gen phishing simulation platform, designed to help Compliance leaders build a more security-conscious and ethically aligned workforce. Embedded within the Catalyst platform, Catalyst Phishing is easy to activate and manage, no technical expertise required.

Rather than relying on outdated, one-size-fits-all training, Catalyst Phishing delivers behavior-based simulations and just-in-time microlearning that creates lasting change across your global workforce. This is a powerful tool for Compliance teams to support culture, behavior, and audit readiness.



Simulate

Model simulations around real employee risk scenarios



Train

Deliver training at the moment of risk, without overwhelming employees



Measure

Demonstrate program impact with easy-to-use reporting



Behavior-based training

- Deliver targeted, just-in-time training triggered by user behavior
- Utilize short, focused training modules to educate users through intuitive, scenario-based narratives



Compliance-ready reporting

- Export data easily for audit, board-level reporting, or executive summaries
- Measure training impact with in-built reporting using level risk analysis and behavior tracking



Premium, modern content

- Access expert developed conversational AI modules for real-world decision-making
- Customize course tone, visuals, and examples to match organizational risk areas



Intuitive admin experience

- Intuitive UI, no HTML or technical skills needed
- Set campaign frequency and let Catalyst automate delivery.



Key features and capabilities

- Real-word simulations
- Behavior-based training
- Flexible campaign management
- 50+ ready-to-use templates
- Built-in campaign reporting and user-level tracking
- Microlearning and premium content
- Security and privacy compliance
- Multilingual simulation delivery
- Seamless integration



How it works

Phishing: Learner experience

This diagram showcases how the credential harvesting Phishing Bundle works. This bundle contains 3 assets: Email, Landing Page and a Phished Page.



Your Password Expires Today

Dear John Doe,

Our records indicate that your corporate password is set to expire by the end of **Aug 29, 2025**. To avoid interruption to your access, please update your password immediately by following the link below:

[Update Password Now](#)

Need help?
Contact [Support Contact](#)

Security Tip:
Always ensure you are updating your password

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Business name

Verify Your Identity

Before updating your password, we need to verify your account.

Email

Current Password

New Password

Confirm New Password

[Continue](#)

Need help? [Contact support](#)

LRN Inspiring Principled Performance Phishing simulation

You took the bait, [NAME]!

You entered personal information into a fake login page as part of a Phishing simulation.

Don't get phished again...

DO verify URLs are genuine before clicking on them.

DO pay attention to what you're clicking.

DON'T enter personal information into a form emailed to you, particularly where there's a sense of urgency.

DO report suspicious emails to your IT department

DO enable Multi-Factor Authorization (MFA).

DON'T click on links that seem suspicious.

Report any suspicious emails to your IT departments.

Step 1: User receives a credential harvesting based phishing simulation and opens email

Step 2: User clicks on 'Update Password Now' and enters their credentials and clicks continue

Step 3: User is redirected to the Phishing Page (just-in-time learning)

