Reduce risk where it matters most, with smarter phishing simulations

Catalyst Phishing is LRN's next-gen phishing simulation platform, built to help security teams reduce human cyber risk through behavior-based training, relevant simulations, and premium microlearning content. Unlike traditional, one-size-fits-all phishing programs, Catalyst Phishing aligns with real-world attack patterns and user behavior, delivering simulations that mirror evolving phishing tactics.

Designed for quick deployment, global scalability, and multilingual support, Catalyst Phishing gives security leaders the tools to improve resilience across their organization.

Simulate

Run smarter simulations that reflect real threats, not just generic lures

Train

Trigger targeted microlearning when risky behavior is detected

Measure

Connect training outcomes to risk reduction and ROI

Real-world phishing simulations

- Simulate current phishing trends and social engineering tactics
- Utilize 50+ customizable phishing templates modeled on spoofed brands and spear phishing

Security & privacy compliance

- GDPR-compliant data handling and EU/US residency options
- No credential data is logged, stored, or monitored

Behavior-based training

- Deliver training when users click a phishing link or enter credentials
- Conversational AI microlearning designed to educate users through intuitive, scenario-based narrative

Seamless integration

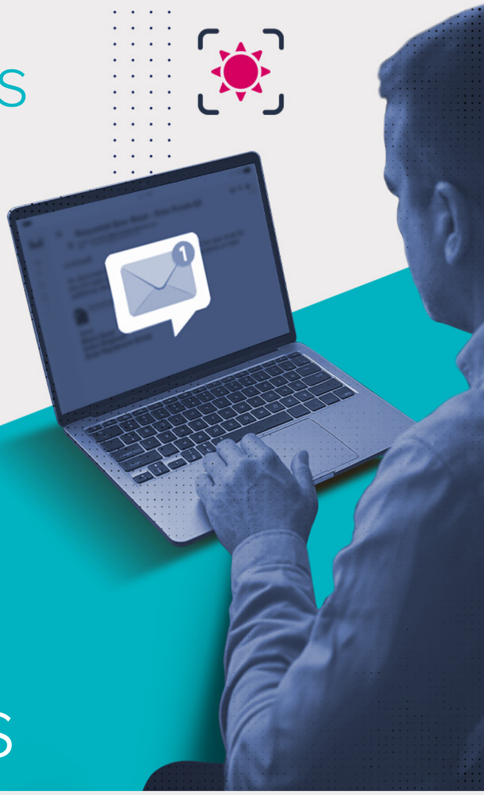
- Manage simulations from a single Catalyst interface
- No separate tools or platform logins required

LRN® *Inspiring Principled Performance®*

LRN.com

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

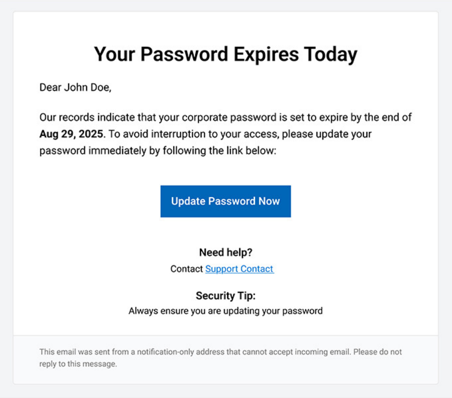


How it works

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.

1 → 2 → 3



Your Password Expires Today

Dear John Doe,

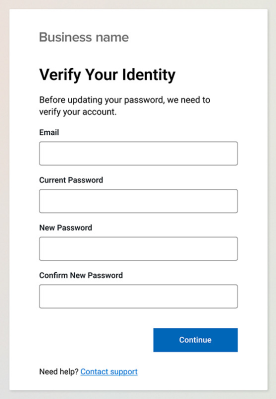
Our records indicate that your corporate password is set to expire by the end of **Aug 29, 2025**. To avoid interruption to your access, please update your password immediately by following the link below:

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.

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



Business name

Verify Your Identity

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

Email

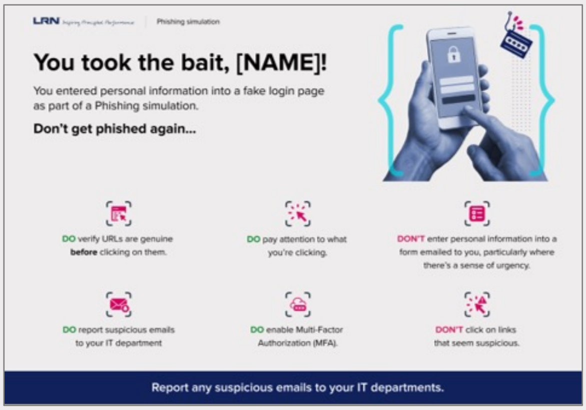
Current Password

New Password

Confirm New Password

Need help? Contact support

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



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

LRN *Inspiring Principled Performance*

LRN.com