

スマートなフィッシングシミュレーションで最重要領域のリスクを軽減

Catalyst Phishingは、LRNの次世代フィッシングシミュレーションプラットフォームです。行動ベースのトレーニング、実際の脅威を取り入れたシミュレーション、優れたマイクロラーニングコンテンツで、人為的なサイバーリスクを減らすことにより、セキュリティチームを支援します。これまでの画一的なフィッシングプログラムと異なり、Catalyst Phishingは実際の攻撃パターンやユーザーの行動に即し、巧妙化するフィッシング手口を反映したシミュレーションを提供します。Catalyst Phishingは、迅速な導入や全社的な拡張が可能で、多言語にも対応もしているため、組織全体の復元力を高めることができます。



シミュレーション

一般的なルアー（おとり）だけでなく実際のフィッシングの脅威を再現したスマートなシミュレーションを実行



トレーニング

リスクのある行為が検知されると、ターゲットを絞ったマイクロラーニングを開始



測定

トレーニングの成果をリスク軽減や投資対効果と照らし合わせて評価



実際のフィッシングを反映したシミュレーション

- フィッシングの最新傾向とソーシャルエンジニアリングの手口をシミュレーション
- 企業ブランドのなりすましやスパイフィッシング(標的型フィッシング)をモデルとした50種類以上のカスタマイズ可能なフィッシングテンプレートを使用



セキュリティ & プライバシーの法準拠

- GDPRに準拠したデータ処理とEU域内/米国内在住者向けのオプション
- 認証情報データの記録、保存、監視なし



行動ベースのトレーニング

- ユーザーによるフィッシングリンクのクリックや認証情報の入力でのトレーニングを開始
- 直感的なシナリオ形式でユーザーを教育する会話形AIマイクロラーニング



シームレスな統合

- Catalystインターフェースだけでシミュレーションの管理が可能
- 他のツールやプラットフォームへのログイン不要



特徴と機能

- 実際のフィッシングの脅威を再現したシミュレーション
- 行動ベースのトレーニング
- フレキシブルなキャンペーン管理
- すぐに使える50種類以上のテンプレート
- キャンペーンレポートとユーザーごとの追跡機能を搭載
- マイクロラーニングと優れたコンテンツ
- セキュリティ&プライバシーの法準拠
- 多言語対応のシミュレーション
- シームレスな統合



仕組み

フィッシング：ユーザーエクスペリエンス

以下の図では、クレデンシャルハーベスティング（認証情報収集）に関するフィッシングトレーニングの仕組みを説明しています。このトレーニングには、メール、ランディングページ、フィッシングページの3種類のステップで構成されています。

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:

[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.](#)

ステップ1: ユーザーはクレデンシャルハーベスティングのフィッシングシミュレーションを受信し、メールを開封する

ステップ2: ユーザーは[パスワードの更新]をクリック認証情報を入力して[次へ]をクリックする

ステップ3: ユーザーはフィッシングページへ転送される（ジャストインタイム学習を開始）

