

Sensibilisez vos équipes aux cybermenaces réelles

➤ **91 % des cyberattaques commencent par un courriel. Vos collaborateurs sauraient-ils repérer la menace ?**

Sensibilisations tout public :

- Hameçonnage, mots de passe et hygiène numérique au quotidien.
- menaces liées au hameçonnage avancé.
- Usage caché de l'intelligence artificielle : risques liés à l'utilisation non encadrée d'outils génératifs.

Sensibilisations techniques par profil :

- Responsables produit : récits utilisateurs sécurisés, récits d'abus, critères d'acceptation.
- Développeurs : principales failles applicatives personnalisées, analyse de code vulnérable, intelligence artificielle et sécurité du code.
- Testeurs et assurance qualité : vérifications de sécurité dans les tests, validation des exigences.

OBJECTIF

Toutes nos sensibilisations sont conçues sur mesure. Nous adaptons les thématiques, le format et la profondeur au contexte de chaque client.

Formation en ligne normalisée :

- Modules sur mesure intégrant votre charte graphique
- Conformité réglementaire : cybersécurité, résilience numérique, cryptoactifs, données personnelles, etc.
- Scénarios engageants : attaques par intelligence artificielle, hypertrucage, hameçonnage vocal
- Compatible avec toutes les plateformes de formation.

Ateliers interactifs :

- Piratage en direct, Hypertrucage, intelligence artificielle pour développeurs.

CAS CONCRET

Sensibilisation annuelle récurrente — Secteur assurance

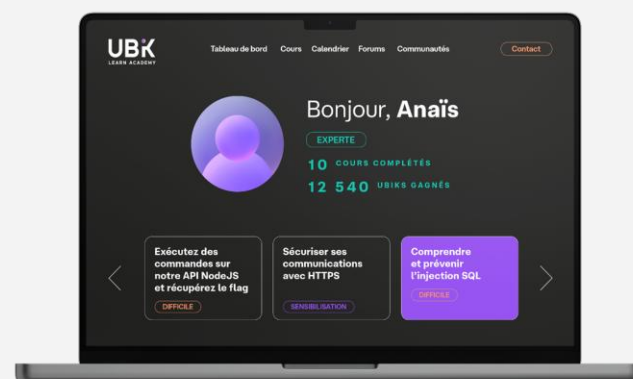
800 collaborateurs par an — cinq cents en français, trois cents en anglais. Trois sessions cette année (fausse correction, logiciel espion, intelligence artificielle). Le contenu évolue avec les menaces.

Formation réglementaire en ligne — Secteur bancaire

Modules réglementaires intégrant la cybersécurité, la résilience numérique, cryptoactifs et la protection des données, avec scénarios engageants hypertrucage et hameçonnage vocal. Déploiement sur la plateforme de formation du client.

Cinq failles applicatives clés et défi dédié — Industrie

Création d'une sélection de cinq failles applicatives propres au client, basée sur les vulnérabilités réellement rencontrées. Cours, travaux pratiques et défi sur mesure pour chaque faille identifiée.



Je vois comme l'attaquant → Je comprends les vulnérabilités → Je me protège

La Roche-sur-Yon

3 rue Vincent Auriol, 85000 La Roche Sur Yon

Paris

43 avenue de Clichy, 75017 Paris

Lyon

20 rue de la Villette, 69003 Lyon

Toulouse

39 rue des Changes, 31000 Toulouse

contact@lexfo.fr

LEXFO.FR