



Profil de l'entreprise



Nous avons une mission très claire

Transformer le comportement des utilisateurs

« Ce n'est qu'ainsi que les entreprises publiques et privées pourront aborder la transition numérique en toute sécurité.

Pour que cela se produise, il est nécessaire que les personnes acquièrent une bonne posture numérique, indispensable pour réduire la composante de vulnérabilité qui découle de l'erreur humaine.

L'acquisition d'une approche consciente des cyber-risques transformera les utilisateurs numériques de maillon faible de la chaîne défensive en première ligne de défense contre la cybercriminalité. »

Security Awareness Training That Works!

Gianni Baroni, fondateur et PDG de Cyber Guru

La sécurité numérique pour l'humanité

Nous sommes convaincus que les technologies numériques contribueront à améliorer de nombreux aspects de notre vie.

Mais nous sommes également convaincus qu'en l'absence d'une attitude correcte dans leur utilisation, il pourrait y avoir plus d'ombres que de lumières.

C'est pourquoi nous nous engageons à rendre l'humanité plus cyber-sécurisée.

Cyber Guru en bref

Security Awareness Training That Works!

Index

À propos de nous



Clients



Où nous trouver



Ce qu'ils disent de nous



Une plateforme de formation complète



Les programmes de formation



Cyber Guru

A été créée en 2017 pour combler le manque d'efficacité des parcours de formation de sensibilisation à la sécurité présents sur le marché.

Depuis 2017, Gianni Baroni est fondateur, PDG et administrateur délégué de la société.

Cyber Guru est aujourd'hui présente en Europe avec sa plateforme de Security Awareness Training la plus efficace, engageante et facile à gérer sur le marché.

Chiffres

> 650,000
Utilisateurs actifs

> 3,5 millions
Leçons suivies

> 4,5 millions
Simulations effectuées

Plus de 500 entreprises nous font déjà nos confiance

Any size, any vertical

Nous aidons nos clients à transformer le comportement numérique de leur main-d'œuvre afin que personne ne puisse devenir un allié inconscient de la cybercriminalité.

C'est pourquoi des entreprises, publiques ou privées, de toute taille et secteur d'activité, sont devenues nos clients.



Fabrication



Formation



Luxe et mode



Électricité et énergie



Administration publique



Santé



Services informatiques



Télécommunications et médias



Banques et assurances



Transports



Commerce de détail



Industrie alimentaire

Nous sommes présents en

Europe :
Italie
France
Espagne

Paris

Campus Cyber
5 Rue Bellini
92800 Puteaux

Milan

Regus Milano Bicocca
Via Libero Temolo 4
20126 Milan

Madrid

Rome

Viale della Grande Muraglia 284
00144 Rome

Ce qu'ils disent de nous

The best Cyber training

“Great product and great team. Easy to implement and with a very proactive support team. No effort to keep it running”

CIO - Manufacturing Industry

★★★★★ - Cyber Guru Security Awareness Training

Really Easy and Effective

“Intuitive solution, easy to use and designed to maximize user attention”

Chief Information Officer - Consumer Goods Industry

★★★★★ - Cyber Guru Security Awareness Training

Cyber Guru is the best solution for Cyber Risk Awareness

“Kind and competent, they are very supportive especially in configuration and optimization activities of IT security solutions”

IT Manager and PMO - Banking Industry

★★★★★ - Cyber Guru Security Awareness Training

Very good product in contents and user experience

“Very good product in contents and user experience. Move the effort regarding awareness from internal team to the product”

Chief Information Security Officer - Energy and Utilities Industry

★★★★★ - Cyber Guru Security Awareness Training

Everything worked perfectly

“All people involved are skilled, committed and available. Our goal - to increase - employees awareness - seems reached”

Manager, IT Security and Risk Management - Manufacturing Industry

★★★★★ - Cyber Guru Security Awareness Training

Great product and support

“We subscribed all the training channels of Cyber Guru platform. It's the perfect training: short and effective lessons, once a month, funny gamification”

Manager, IT Security and Risk Management - Transportation Industry

★★★★★ - Cyber Guru Security Awareness Training



Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose

Security Awareness Training : une plateforme complète

La plateforme Cyber Guru est conçue pour optimiser l'efficacité des processus d'apprentissage et consolider au fil du temps la prise de conscience nécessaire pour faire face à l'évolution continue des techniques utilisées par les cybercriminels.

L'objectif principal des programmes de formation est d'influencer le comportement des utilisateurs en développant les trois principales caractéristiques défensives de chaque individu : la connaissance, la perception du danger et la promptitude.

Ce n'est qu'en travaillant simultanément sur ces caractéristiques qu'il est possible d'activer ce processus de transformation des comportements, essentiel dans un programme de formation réellement efficace.

C'est pourquoi la plateforme offre une formation complète basée sur trois programmes méthodologiques : COGNITIF, INDUCTIF, EXPÉRIENTIEL.

Une plateforme,
trois programmes de
formation



Méthodes de formation

Formation **Cognitive** La connaissance

La connaissance est développée à travers un programme de formation cognitive, Awareness Training, basé sur une approche principalement didactique qui agit sur la partie du cerveau la plus rationnelle. Ce programme explique les principaux types de menaces, comment elles se concrétisent et quelles sont les logiques comportementales les plus appropriées à suivre.

Formation **Inductive** La perception du danger

La capacité à percevoir le danger, nécessaire pour reconnaître une menace, se développe à travers un programme de formation inductive. La Channel Training utilise la narration de situations réelles pour affecter la composante émotionnelle de notre cerveau. L'apprenant, en se plongeant dans l'histoire, peut comprendre comment n'importe qui peut devenir victime de la cybercriminalité.

Formation **Expérientielle** La promptitude

Pour réagir rapidement en adoptant le bon comportement face à l'apparition d'un danger, il est nécessaire de continuer de s'entraîner à la promptitude grâce à des simulations d'attaque d'hameçonnage ou d'hameçonnage par SMS. Le programme de formation de Phishing Training est réalisé pour former cette partie du cerveau qui est par nature prédisposée à activer les mécanismes d'action-réaction.

Les trois programmes de formation



Cyber Guru Awareness

Le programme d'enseignement cognitif, basé sur une méthodologie de formation continue, assure le développement progressif de la sensibilisation grâce à la connaissance des menaces du réseau et des comportements à adopter pour prévenir les attaques.



Cyber Guru Channel

Le programme de formation inductive qui, grâce à la force d'un schéma narratif typique des séries télévisées, génère chez l'apprenant la capacité à apprendre par l'identification dans des situations réelles.



Cyber Guru Phishing

Le programme d'entraînement expérientiel automatique et adaptatif, avec fonction anti-hameçonnage, permet un entraînement personnalisé basé sur les expériences individuelles et le niveau unique de résistance aux attaques.

Cyber Guru Awareness

Cyber Guru Awareness est la composante didactique de la plateforme, en mode e-learning, qui s'occupe de développer une formation purement cognitive. L'objectif principal de cette programme est de développer la connaissance des cyber-menaces. Un processus d'apprentissage progressif, suivi du maintien des connaissances et de la mise à jour des compétences.



Modules de formation auto-cohérents avec activation mensuelle



Engagement hebdomadaire minimal, compatible avec toutes les fonctions



Micro leçons vidéo au format multimédia



Utilisation d'acteurs professionnels ayant des fonctions de coach



Langage très vulgarisant



Approche interactive avec une alternance continue entre les micro leçons et les tests



Questionnaire d'évaluation à choix multiples



Méthodologie de ludification, avec organisation en équipe



Plateforme multilingue



Contenu supplémentaire et constamment mis à jour

Cyber Guru Channel

La méthodologie inductive utilisée est basée sur l'immersion de l'utilisateur dans une situation réelle et sur un processus d'auto-identification avec la cyber-menace, qui prend donc une forme concrète. L'utilisateur prend conscience non pas à travers une notion, mais à travers une narration, qui agit d'abord sur la perception du danger, puis sur l'élément conceptuel, en dépassant une arrière-pensée très dangereuse : « cela ne peut pas m'arriver ». Les trois principales caractéristiques sont l'apprentissage inductif efficace, l'implication maximale de l'apprenant et la supervision à impact zéro.



Formation continue



Production vidéo avancée



Plusieurs formats vidéo avec différentes narrations



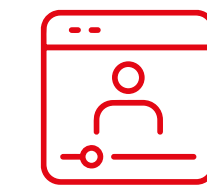
Épisodes courts



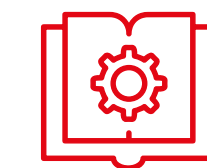
Rythme narratif élevé



Auto identification dans des situations réalistes



Approche Netflix-Like



Documentation détaillée pour chaque épisode



Reporting complet sur le niveau d'utilisation



Fonctions de student caring automatique, pour motiver la participation

Cyber Guru Phishing

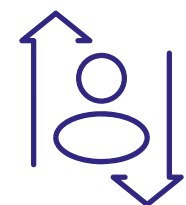
Cyber Guru Phishing a été conçue pour former le personnel à résister aux attaques d'hameçonnage, par le biais de campagnes d'attaques simulées, personnalisées sur la base du profil comportemental de l'utilisateur individuel, grâce à un processus automatique et adaptatif, guidé par l'utilisation de technologies d'intelligence artificielle. L'apprenant augmente la résistance aux attaques par l'expérience, à la fois celle négative de l'erreur et celle positive de la reconnaissance de l'attaque. Les trois principales caractéristiques sont l'entraînement expérientiel efficace, l'entraînement personnalisé et la supervision sans impact.



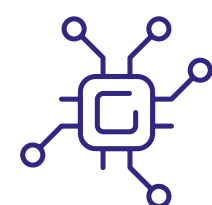
Entraînement expérientiel efficace et continu



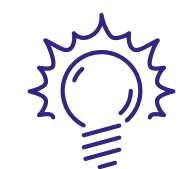
Entraînement personnalisé par processus adaptatif



Niveaux de difficulté et simulations personnalisées



Campagnes d'attaque automatisées



Erreur > Formation instantanée



Procédure d'alerte



Modèles préchargés



Rapports analytiques et managériaux via un tableau de bord avancé



Groupes à risque



Politiques de remédiation



Security Awareness Training That Works!

www.cyberguru.io