

SCIENCES, TECHNOLOGIES, SANTÉ

Formation courte - Sensibilisation à la cybersécurité

**Durée**
4 heures**Langue(s)
d'enseignement**
Français**Composante**
Direction
formation
professionnelle
et
apprentissage

Présentation

L'essor des cybermenaces expose les TPE et PME à des risques majeurs (vol de données, rançongiciels, phishing, etc.). Ces entreprises, souvent dépourvues d'un service dédié à la cybersécurité, manquent d'une sensibilisation et de compétences internes pour faire face à ces enjeux. Face à ce constat, notre formation vise à doter toutes personnes de l'entreprise utilisant un outil du SI (Système informatique) d'assurer un premier niveau de protection et de gestion des risques cyber.

Objectifs

Cette formation a pour objectifs de permettre aux utilisateurs de systèmes informatiques (ordinateurs, tablettes, téléphones...) d'identifier les cybermenaces de plus en plus fréquentes et de mettre en place de bonnes pratiques au quotidien.

Compétences visées

Vous serez capable à l'issue de ces 4 heures de :

- Comprendre les enjeux essentiels de la cybersécurité
- Reconnaître les principales menaces
- Appliquer les bonnes pratiques au quotidien

- Savoir réagir face à un incident

Admission

Public cible

Cette formation s'adresse à toutes personnes de l'entreprise utilisant un outil du SI, non spécialistes n'ayant pas forcément la "fibre cyber".

Modalités de candidature

- Dossier de candidature à télécharger.
- Merci de renvoyer votre dossier complété au service de la formation continue: formation.continue@cyu.fr
- Les candidatures sont traitées par ordre d'arrivée, nous vous invitons donc à nous faire parvenir votre dossier au plus tôt.

Droits de scolarité

220 € (financement individuel)

280 € (formation financée par un tiers)



Dimension internationale

Maison des langues

La Maison des langues propose différents services (cours de langues, ateliers de conversation, entraînements aux certifications, tests de positionnement, passage du Toeic) pour vous aider à progresser en langues et à obtenir une certification reconnue, quels que soient votre parcours et votre niveau. Des dispositifs spécifiques sont prévus selon les formations.

 En savoir plus sur la maison des langues

Infos pratiques

Contacts

Victoria Nguyen

 0134256332

 Victoria.nguyen3@cyu.fr

Cynthia Bockler

 06 24 09 23 25

 formation.continue@cyu.fr



Programme

Organisation

4 heures de formation en distanciel

Prochaine date de formation disponible : 27 mars 2026

Intervenant :

Nicolas Thore, diplômé en gestion de projet informatique, a toujours été passionné par l'innovation numérique. C'est en occupant des postes de Directeur des Systèmes d'information dans des secteurs sensibles tels que le médical ou la sûreté internationale qu'il a développé une expertise dans la protection des infrastructures informatiques.

Lors de la crise COVID-19, il prend la mesure des vulnérabilités auxquelles sont confrontées les TPE/PME. Il fonde GUIDDY après avoir constaté que ces petites entreprises étaient souvent démunies face aux cybermenaces.

Aujourd'hui, il souhaite apporter des solutions accessibles et personnalisées pour ces entreprises, avec une ambition claire : démocratiser la cybersécurité.

Contenu de la formation

Module 1 : La Cybersécurité (9h - 9h45) Comprendre les enjeux de la cybersécurité pour une entreprise et identifier les formes courantes de cyberattaques

- Pourquoi la cybersécurité nous concerne tous
- Quelques chiffres cyber
- Exemple Cyberattaque
- Une nouvelle économie

Module 2 : Les Principales Menaces (9h45 - 10h30) Identifier les principales formes d'attaques

- Phishing
- Attaque DDOS
- Arnaque au président
- Ingénierie Sociale
- L'humain
- QCM

Module 3 : Les bons réflexes (10h30 - 11h15) Mettre en œuvre les bonnes pratiques numériques pour réduire les risques quotidiens

- Mot de passe
- Sauvegardes
- Pièges quotidiens (wifi publics, clé usb, mise à jour...)



- Pro/Perso
- Réseaux Sociaux
- Cloud
- Télétravail et mobilité

Module 4 : Gestion de crise (11h15 - 11h45) Comprendre les étapes d'une gestion de crise cyber et adopter les bons réflexes face à une cyberattaque

- PCA
- PRA
- Comment réagir en cas de cyberattaques
- Premiers gestes

Module 5 : Obligations Légales & conformité (11h45 - 12h15) Identifier les obligations légales en matière de cybersécurité et les implications concrètes pour l'entreprise :

- RGPD
- CNIL / ANSSI / Cybermalveillance
- NIS2
- QCM

Module 6 : Cas pratique et Echange (12h15- 13h) Appliquer les connaissances acquises à travers une mise en situation pratique pour renforcer la mémorisation des réflexes à adopter.

Méthodologie

- Cours théoriques (cybersécurité) avec participation des apprenants
- QCM
- Supports de formation
- Cas concrets, exemples pratiques

