Introduction à la sécurité des projets web

e-learning (1 jour)

# Consignes

**1 journée en e-learning**. Vous pouvez aborder les contenus à votre rythme mais être **obligatoirement connectés** à la classe virtuelle TEAMS entre 9h30 et 17h30.

* **Pensez à émarger !**

A vos claviers ou stylos ! Une fiche de synthèse sera la bienvenue pour votre mémorisation 😊 !

Nous vous invitons fortement à échanger avec vos pairs sur Teams, poser vos questions, partager vos difficultés éventuelles et faire les exercices proposés.

# Qu’est-ce la sécurité informatique et la Cybersécurité ?

La sécurité informatique et la cybersécurité sont deux domaines cruciaux dans le paysage technologique contemporain, essentiels pour protéger les données, les systèmes et les utilisateurs contre les menaces numériques. La sécurité informatique englobe un large éventail de pratiques, de politiques et de technologies visant à garantir la confidentialité, l'intégrité et la disponibilité des données stockées et traitées par les systèmes informatiques. Cela implique la mise en place de mesures de sécurité telles que l'authentification des utilisateurs, le chiffrement des données, la gestion des accès et la surveillance des activités suspectes.

D'autre part, la cybersécurité se concentre spécifiquement sur la protection des réseaux, des systèmes et des données contre les attaques informatiques malveillantes. Cela inclut la prévention des intrusions, la détection des menaces, la réponse aux incidents et la récupération après une attaque. Les professionnels de la cybersécurité travaillent à la mise en place de pare-feu, de systèmes de détection d'intrusion, de solutions antivirus et de politiques de sécurité robustes pour contrer les cybermenaces toujours évolutives.

Ensemble, la sécurité informatique et la cybersécurité sont essentielles pour protéger les organisations, les gouvernements et les individus contre une gamme variée de risques numériques, tels que les logiciels malveillants, les attaques par phishing, les ransomwares, les violations de données et les cyberattaques sophistiquées. En adoptant une approche proactive et en restant à jour avec les dernières technologies et les meilleures pratiques de sécurité, il est possible de réduire considérablement les risques et de garantir la sécurité et la confidentialité des informations sensibles dans le monde numérique en constante évolution.

# Les ressources à consulter

## Les fondements de la sécurité informatique et de la cybersécurité.

|  |  |
| --- | --- |
|  | **Objectifs de la séance**  A la fin de cette séance, vous serez capables de :   * Réaliser un état des lieux de la cybersécurité * Évaluer les menaces des malwares * Comprendre l’ingénierie sociale * Protéger son poste de travail et suivre les bonnes pratiques |

**Ressource LinkedIn Learning :** [**visionnez.**](https://www.linkedin.com/learning/les-fondements-de-la-securite-informatique-et-de-la-cybersecurite)

**Durée :** 1h 47min

**Formateurs :**

* Pierre Cabantous – Intégrateur de solutions réseaux

**Résumé :**

Les bases de données informatiques sont sensibles aux attaques et peuvent être accessibles par n'importe qui. Êtes-vous préparé à ces menaces ? Quel est le niveau de sécurité de votre poste de travail chez vous ou dans votre entreprise ? Dans ce cours, Pierre Cabantous vous propose de comprendre la cybersécurité et évoque avec vous les risques que vous encourez, avec ou sans connexion réseau. Ensemble, vous étudierez les types d'attaques menées par les pirates pour voler vos informations personnelles, vous escroquer ou contrôler votre machine à distance. Vous verrez comment fonctionne un virus et comment les hackers vous manipulent avec des techniques d'ingénierie sociale. À l'issue de ce cours, vous serez en mesure de vous protéger à l'aide d'antivirus et des bonnes pratiques de sécurité informatique.

**QCM à réaliser :**

Examen : 289119

Lien vers le QCM n°1: <https://evalbox.com/register/exam/code/PXUVG>

## [La sécurité informatique et cybersécurité : Niveau avancé](https://www.linkedin.com/learning/la-securite-informatique-et-cybersecurite-niveau-avance?contextUrn=urn%3Ali%3AlyndaLearningPath%3A61b33595498e6976674cae51&u=123653769)

|  |  |
| --- | --- |
|  | **Objectifs de la séance**  A la fin de cette séance, vous serez capables de :   * En savoir plus sur les risques et principales attaques informatiques. |

**Ressource LinkedIn Learning :** [**visionnez.**](https://www.linkedin.com/learning/la-securite-informatique-et-cybersecurite-niveau-avance?contextUrn=urn%3Ali%3AlyndaLearningPath%3A61b33595498e6976674cae51&u=123653769)

**Durée :** 2h02m

**Formateurs :**

* Pierre Cabantous – Intégrateur de solutions réseaux

**Résumé :**

En tant que responsable de la sécurité ou DSI, vous devez mettre en place une politique de cybersécurité pour répondre aux menaces qui pèsent sur votre informatique. Pour cela, Pierre Cabantous vous propose de faire un tour de la cybersécurité en entreprise. Dans ce cours, vous étudierez la démarche d'un pirate, avant et après l'intrusion dans un système, à la suite de l'exploitation d'une vulnérabilité. Vous verrez comment gérer ces vulnérabilités par rapport à un niveau de risque que vous apprendrez à calculer. Vous aborderez aussi une des principales menaces encourues aujourd'hui par tout service accessible en ligne : les attaques par déni de service. Puis vous découvrirez comment protéger votre organisation aux niveaux technique et organisationnel, en suivant des bonnes pratiques, des process ainsi que des normes européennes comme le RGPD.

**QCM à réaliser :**

Examen : 313435

Lien vers le QCM: <https://evalbox.com/register/exam/code/RN5YQ>