TU ES COLLÉGIEN OU LYCÉEN ?

LA CYBERSÉCURITÉ T'INTRIGUE ?

Laisse-nous t'éclairer sur ce secteur en pleine expansion et sur les formations qui pourront t'y former.

CYBERSCHOOL
ÉCOLE UNIVERSITAIRE
DE RECHERCHE EN CYBERSÉCURITÉ

SOMMAIRE

1 LA CYBERSÉCURITÉ, C'EST QUOI ?

Un enjeu crucial pour notre société

La cybersécurité, c'est l'ensemble des **mesures, pratiques, technologies et stratégies mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les menaces numériques.**

Pourquoi est-elle si essentielle ?

1. Pour protéger nos informations personnelles : La cybersécurité veille à ce que nos coordonnées, numéros de sécurité sociale ou encore informations financières, souvent stockées en ligne, restent privées et en sécurité.

2. Pour assurer la confidentialité des données : En garantissant que seules les personnes autorisées peuvent accéder aux informations et en protégeant contre les modifications non autorisées, la cybersécurité assure que nos données restent fiables et intègres.

3. Pour prévenir les interruptions de services : Les cyberattaques peuvent rendre des sites web et des services importants inaccessibles, causant des perturbations majeures pour les entreprises et les organisations.

4. Pour réagir aux incidents de sécurité : Avec de bonnes pratiques en place, les organisations sont prêtes à détecter, réagir et se remettre rapidement des incidents de sécurité. Elles intègrent la sécurité numérique dans la conception de leurs produits et services pour garantir une protection maximale à leurs utilisateurs et sensibiliser davantage leurs collaborateurs.

Des métiers prometteurs et dynamiques

La cybersécurité offre un **panel impressionnant de métiers et de domaines de spécialisation**, qui ne va cesser d'augmenter. Le secteur est en plein essor, avec de nombreuses entreprises, start-ups et laboratoires de recherche dédiés à la cybersécurité présents sur le territoire rennais, et plus globalement breton. **Rennes attire, recrute et devient incontournable en matière de cybersécurité.**

Travailler dans la cybersécurité, c'est :
- **Collaborer en réseau** avec des collègues passionnés.
- **Apprendre en continu** et rester curieux des dernières innovations.
- **Contribuer à des projets innovants** dans un domaine en pleine expansion.

Si tu es curieux des nouvelles technologies, aime résoudre des problèmes complexes, et veux jouer un rôle crucial dans la protection des systèmes informatiques, **la cybersécurité pourrait être la voie idéale pour toi !**

2 DÈS LE LYCÉE

Le baccalauréat général te permet d'accéder à des formations post-bac qui te formeront au secteur de la cybersécurité. Pour te préparer au mieux, nous te recommandons de sélectionner une ou plusieurs de ces spécialités :

- **Numérique et Sciences Informatiques (NSI) :** si tu souhaites résoudre des problèmes complexes, concevoir des programmes, comprendre les algorithmes et les systèmes informatiques.
- **Mathématiques :** si tu es intéressé par les aspects théoriques et pratiques des mathématiques, comme la cryptographie, les algorithmes, ou la modélisation.
- **Sciences de l'Ingénieur :** si tu es curieux de savoir comment les systèmes sont conçus, testés et améliorés.
- **Physique Chimie :** si tu t'intéresses aux principes physiques et chimiques derrière les technologies, les réseaux ou les dispositifs électroniques.
- **Histoire-Géographie, Géopolitique et Sciences Politiques :** si tu souhaites comprendre les enjeux géostratégiques et les impacts des cybermenaces à l'échelle mondiale, ainsi que les aspects juridiques et politiques de la cybersécurité.

Le baccalauréat technologique Sciences et Technologies de l'Industrie et du Développement Durable (STI2D) spécialité Systèmes d'Information et Numérique (SIN) est également une très bonne option si tu envisages une voie plus technique et que tu souhaites comprendre comment fonctionnent les objets techniques et les réseaux.

Le baccalauréat professionnel Cybersécurité, Informatique et réseaux, ELectronique (CIEL) est également une possibilité si tu aimes les aspects techniques des systèmes informatiques et que tu souhaites apprendre à protéger ces infrastructures contre les cyberattaques.

3 TES ÉTUDES SUPÉRIEURES EN CYBERSÉCURITÉ

LE BREVET DE TECHNICIEN SUPÉRIEUR (BTS)

Le **BTS** est un cursus de 2 ans qui permet d'acquérir les connaissances et compétences nécessaires pour intégrer une troisième année de licence à l'université, une troisième année de BUT ou certaines écoles d'ingénieurs. Tu peux aussi opter pour une entrée dans le monde du travail.

L'admission en BTS se fait via la plateforme en ligne *Parcoursup*.

Voici deux BTS que nous te recommandons :

- **BTS Services Informatiques aux Organisations (SIO)**
- **BTS Cybersécurité, Informatique et réseaux, ELectronique (CIEL)**

Si tu souhaites poursuivre tes études après ton BTS, nous te conseillons de te renseigner sur les prérequis de l'établissement qui t'intéresse pour ta troisième année post-bac, afin de choisir le BTS le mieux adapté.

LA CLASSE PRÉPARATOIRE AUX GRANDES ÉCOLES (CPGE)

La **Classe Préparatoire aux Grandes Écoles** est un cursus de 2 ans qui permet d'accroître les connaissances des bacheliers dans différents domaines disciplinaires, dans le but d'intégrer par la suite une école d'ingénieurs, une grande école ou un cursus universitaire.

L'admission pour une CPGE se fait via la plateforme en ligne *Parcoursup*.

Nous te recommandons de choisir une **CPGE scientifique**.

LE BACHELOR UNIVERSITAIRE DE TECHNOLOGIE (BUT)

Le **BUT**, qui est une formation en 3 ans, peut te permettre d'accéder au secteur de la cybersécurité.

L'admission en BUT se fait via la plateforme en ligne *Parcoursup*.

L'**IUT de Saint-Malo et l'IUT de Lannion** proposent par exemple le **BUT Réseaux & Télécommunication** avec une **spécialisation en cybersécurité en deuxième année**. À la suite de ces 3 ans, tu pourras soit intégrer le monde professionnel, soit poursuivre tes études en écoles d'ingénieurs ou à l'université.

L'ÉCOLE D'INGÉNIEURS OU LA GRANDE ÉCOLE

Les **écoles d'ingénieurs** et les **grandes écoles** forment les étudiants sur un cursus de 3 ans à 5 ans (intégration après le bac ou après une CPGE, une licence, un BTS ou un BUT en fonction des établissements).

L'admission à une école d'ingénieurs ou une grande école dépend du niveau d'entrée :

- L'admission après le bac se fait principalement via la plateforme en ligne *Parcoursup*. Elle peut aussi se faire via un concours, examen du dossier et/ou entretien. Tout dépend de l'établissement.

▸ L'admission après une CPGE, une licence, un BTS ou un BUT se fait via un concours, examen du dossier et/ou entretien. Là encore, tout dépend de l'établissement.
Nous te conseillons de consulter les conditions d'admission de l'établissement qui t'intéresse.

Voici quelques exemples d'écoles d'ingénieurs qui forment au secteur de la cybersécurité :

- **INSA Rennes : Diplôme d'ingénieur spécialité informatique option sécurité**
- **IMT Atlantique : Formation Ingénieur généraliste thématique d'approfondissement cybersécurité // Formation Ingénieur par apprentissage spécialité informatique, réseaux, télécommunications**
- **Enssat : Formation ingénieur informatique par apprentissage, cybersécurité, science des données et du multimédia, intelligence artificielle // Formation ingénieur informatique, cybersécurité, intelligence artificielle, science des données, développement logiciel**
- **CentraleSupélec : Diplôme d'ingénieur informatique mention cybersécurité // Diplôme d'ingénieur parcours InfoSec**
- **ESIR : Formation d'ingénieur spécialité informatique**

Concernant les grandes écoles, le **Master Sécurité, défense et intelligence stratégique** de **SciencesPo Rennes** permet de te former à l'aspect géopolitique et géostratégique de la cybersécurité.

L'UNIVERSITÉ

Tout d'abord, tu intègres une **licence** pendant 3 ans, puis tu as le choix entre poursuivre en **master** à l'**université** pendant 2 ans (parcours classique) ou intégrer une **école d'ingénieurs** ou une **grande école**.

L'admission en licence se fait via la plateforme en ligne *Parcoursup*.

Plusieurs possibilités s'offrent à toi, selon ton profil et tes envies, et notamment :

- **La licence Informatique**
- **La licence Électronique**
- **La licence Mathématiques**

La sécurité numérique est un domaine qui se développe également fortement dans le droit et de plus en plus d'offres de formations combinent droit et sécurité numérique. Ainsi, une approche juridique et/ou en sciences politiques représente aussi une très belle option de carrière.

Voici donc deux autres possibilités de licences :

- **La licence Droit**
- **La licence Science politique**

Tu peux effectuer une licence dans n'importe quelle université. Sache que l'**Université de Rennes** propose ces cinq licences mentionnées ci-dessus.

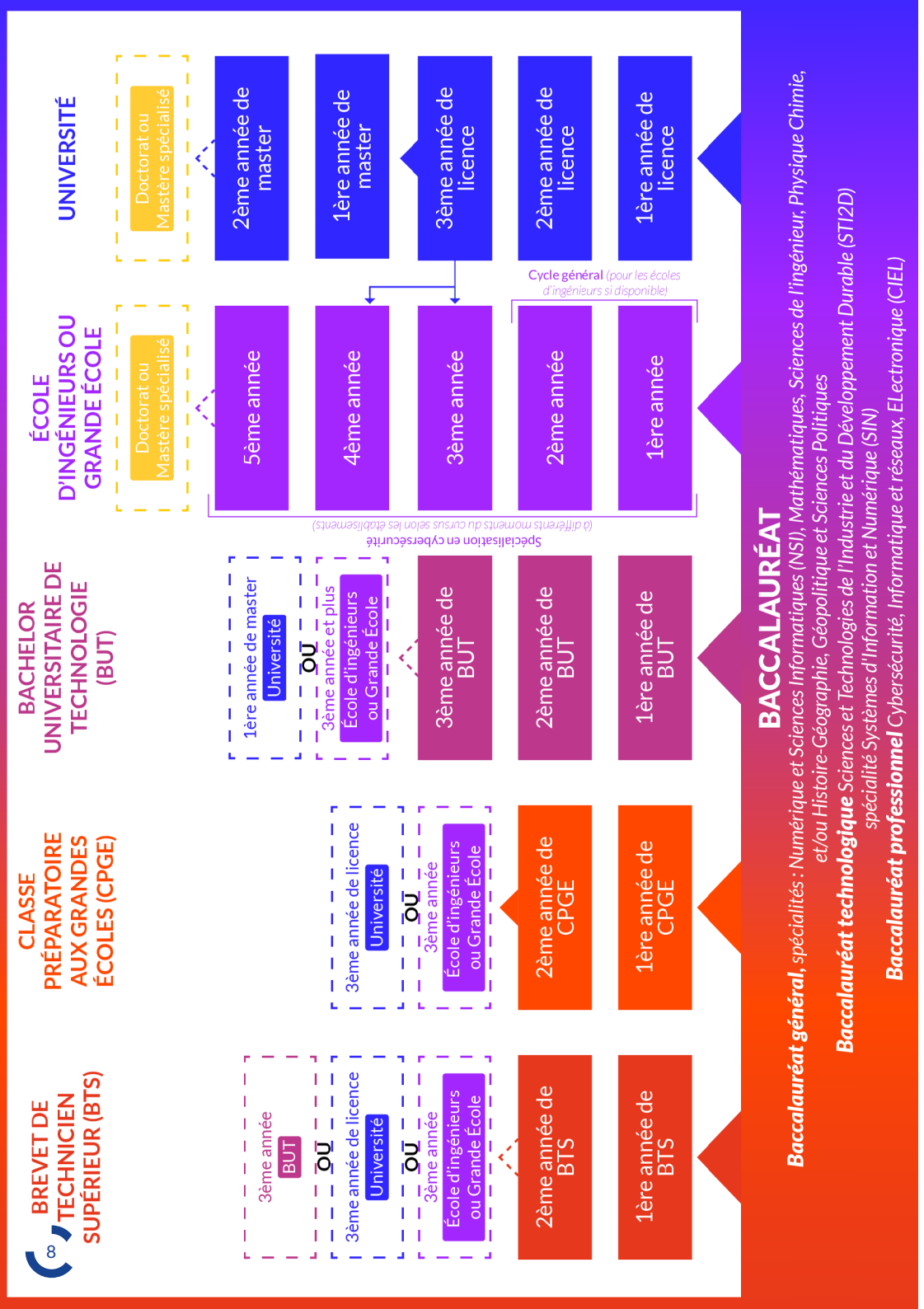
L'admission en master se fait via la plateforme en ligne *Mon Master*.

Voici quelques masters qui forment aux métiers en cybersécurité :

- **Master cybersécurité parcours sécurité logicielle et matérielle**
- **Master cybersécurité parcours Responsable de la Sécurité des Systèmes d'Information**
- **Master mathématiques et applications parcours mathématiques de l'information, cryptographie**

Si tu as choisi de t'orienter vers le droit et la sécurité numérique, tu peux par exemple choisir de poursuivre tes études en **Master droit privé parcours droit du numérique**.

Ces masters sont enseignés à l'**Université de Rennes**. Tu y accèdes notamment via les licences mentionnées ci-dessus.



4 QUELS MÉTIERS EN CYBERSÉCURITÉ ?

La cybersécurité est un domaine complexe et dynamique qui englobe une variété de métiers, chacun jouant un rôle crucial dans la protection des systèmes informatiques et des données. Voici un aperçu des principaux champs d'application dans la cybersécurité :

- **La gestion de la sécurité et pilotage des projets de sécurité :** cette partie s'occupe de la création et de la mise en place des règles et des plans pour protéger les systèmes informatiques. Cela comprend la gestion des projets qui visent à améliorer la sécurité, comme définir les politiques de sécurité et évaluer les risques pour savoir où des protections supplémentaires sont nécessaires.
- **La conception et maintien d'un système d'information sécurisé :** ici, l'objectif est de construire des systèmes informatiques qui sont bien protégés contre les attaques. Cela inclut la création de la structure de sécurité, comme installer des pare-feu (des barrières de sécurité numériques) et des systèmes pour détecter les intrusions. Il faut aussi régulièrement vérifier et mettre à jour ces protections pour rester efficace contre les nouvelles menaces.
- **La gestion des incidents et des crises de sécurité :** quand une attaque ou un problème de sécurité se produit, il faut réagir rapidement. Cette partie s'occupe de détecter les problèmes, de comprendre ce qui s'est passé et de prendre les mesures nécessaires pour résoudre le problème. Elle prépare aussi des plans pour se remettre après une attaque afin de minimiser les dégâts.
- **Le conseil, les services et la recherche :** les experts de ce domaine aident les entreprises à améliorer leur sécurité en leur donnant des conseils, en réalisant des audits de sécurité et en évaluant les vulnérabilités. Ils mènent aussi des recherches pour développer de nouvelles technologies et méthodes pour contrer les cybermenaces et améliorer la cybersécurité.

Selon la formation que tu auras choisie, tu pourras accéder à plusieurs métiers de ces catégories. Tu pourras aussi faire le choix de continuer en doctorat et t'épanouir dans le monde de la recherche.

TESTE TES CONNAISSANCES EN CYBERSÉCURITÉ !

1 Quel est le but d'un ransomware ?

a) Il améliore la performance de l'ordinateur en nettoyant les fichiers inutiles.
b) Il crypte les fichiers de l'ordinateur et demande une rançon pour les débloquer.
c) Il met à jour automatiquement tous les logiciels pour les rendre plus sûrs.

Réponse correcte : b
Les ransomwares sont des types de logiciels malveillants conçus pour bloquer l'accès aux fichiers d'un ordinateur en les cryptant. Les victimes reçoivent alors une demande de rançon pour obtenir la clé de décryptage et récupérer leurs fichiers.

2 Quel signe peut indiquer qu'un e-mail est une tentative de phishing ?

a) L'e-mail provient d'une adresse inconnue, mais semble contenir des informations intéressantes.
b) Le message contient des erreurs de grammaire ou d'orthographe et demande des informations personnelles ou des identifiants de connexion.
c) L'e-mail est envoyé en dehors des heures de bureau habituelles.

Réponse correcte : b
Les tentatives de phishing cherchent souvent à tromper les gens en se faisant passer pour des entreprises ou des institutions légitimes. Les erreurs de grammaire ou d'orthographe sont souvent des signes de faux messages, et ces e-mails demandent généralement des informations sensibles comme des mots de passe ou des coordonnées bancaires.

3 En matière de sécurité des mots de passe, qu'est-ce que la "multi-authentification" ?

a) La vérification en plusieurs étapes pour accéder à un compte, souvent combinant mot de passe et code envoyé par SMS ou email.
b) L'utilisation de plusieurs mots de passe pour différents comptes.
c) Le changement régulier de mots de passe.

Réponse correcte : a
La multi-authentification renforce la sécurité des comptes en ligne en exigeant plusieurs vérifications pour l'accès. En plus du mot de passe, elle peut inclure un code envoyé par SMS ou une empreinte digitale. Cela rend plus difficile pour les attaquants d'accéder à un compte même s'ils connaissent le mot de passe.

4 Quel est le but principal d'un test de pénétration (pentest) ?

a) Augmenter la vitesse de traitement des données en optimisant le réseau.
b) Mettre à jour les logiciels pour corriger les vulnérabilités connues.
c) Identifier les failles de sécurité en simulant une attaque sur le système.

Réponse correcte : c
Un test de pénétration, ou pentest, a pour but de découvrir les vulnérabilités d'un système en simulant des attaques réelles. Cela aide les entreprises à identifier et corriger les failles de sécurité avant que des attaquants malveillants ne puissent les exploiter.

5 Que signifie l'acronyme DDoS en cybersécurité ?

a) Distributed Denial of Service
b) Digital Data of Security
c) Dynamic Defense of Servers

Réponse correcte : a
DDoS signifie "Distributed Denial of Service" (Déni de Service Distribué). Il s'agit d'une attaque où plusieurs ordinateurs sont utilisés pour envoyer un volume massif de requêtes à un serveur. Cela peut causer des interruptions de service, ralentir le site web, et empêcher les utilisateurs légitimes d'y accéder.

6 Quel est l'objectif principal d'une politique de sécurité de l'information ?

a) Assurer un accès illimité à toutes les données.
b) Définir les règles pour protéger les informations contre les menaces et les accès non autorisés.
c) Augmenter la vitesse de traitement des données.

Réponse correcte : b
Une politique de sécurité de l'information établit des règles et des procédures pour protéger les données et les systèmes contre les menaces, les accès non autorisés et les pertes. Elle vise à garantir que les informations sensibles sont sécurisées et que les pratiques de sécurité sont suivies au sein de l'organisation.

7 Qu'est-ce que le social engineering en cybersécurité ?

a) Une technique pour améliorer les performances des réseaux informatiques.
b) Un processus pour installer des mises à jour de sécurité automatiquement.
c) Une méthode pour tromper les gens et obtenir des informations confidentielles par manipulation psychologique.

Réponse correcte : c
Le social engineering est une technique utilisée par les attaquants pour manipuler les individus afin qu'ils divulguent des informations sensibles ou accèdent à des systèmes protégés. Cela implique souvent des manipulations psychologiques, comme se faire passer pour une personne de confiance ou utiliser des tactiques de persuasion pour tromper les victimes.

8 Quel est le principal objectif d'un cheval de Troie ?

a) Optimiser la vitesse du système en supprimant les fichiers inutiles.
b) Réparer les fichiers corrompus et améliorer la sécurité du système.
c) Se déguiser en programme légitime pour tromper les utilisateurs et provoquer des dommages.

Réponse correcte : c)
Un cheval de Troie se présente comme un programme légitime pour tromper les utilisateurs. Une fois installé, il peut permettre aux attaquants d'accéder au système, voler des informations ou causer des dommages.

Bravo d'avoir terminé ce quiz ! La cybersécurité est un domaine complexe mais fascinant. **Continue à explorer et à apprendre pour devenir un expert en cybersécurité !**

CYBERSCHOOL

ÉCOLE UNIVERSITAIRE
DE RECHERCHE EN CYBERSÉCURITÉ

La CyberSchool est la seule École Universitaire de Recherche (EUR) en cybersécurité en France. Elle regroupe des **formations universitaires, d'ingénieurs et de grandes écoles (du bac+1 au bac+8) dispensées par un ensemble d'établissements partenaires, au cœur de la Bretagne.** Les diplômés deviennent des experts, ingénieurs et/ou scientifiques, dans les domaines clés de la cybersécurité.

CYBERSCHOOL
Campus de Beaulieu
263 Av. Général Leclerc
35042 Rennes
E : cyberschool@univ-rennes.fr

Plus d'infos sur notre site internet :
cyberschool.univ-rennes.fr

Avec le soutien de :