Procédure d'utilisation et de sécurisation - Discord

Discord est un logiciel propriétaire gratuit de VoIP (La **voix sur IP**, ou « **VoIP** » pour *Voice over IP*, est une technique qui permet de transmettre la voix sur des réseaux IP filaires (câble/ADSL/fibre optique) ou non (satellite, Wi-Fi et réseaux mobiles), qu'il s'agisse de réseaux privés ou d'Internet.) conçu initialement pour les communautés de joueurs. Il fonctionne sur les systèmes d'exploitation Windows, macOS, Linux, Android, iOS ainsi que sur les navigateurs web. La plateforme comptabilise le 21 juillet 2019 plus de 250 millions d'utilisateurs.

Discord est né en 2015 de Jason Citron avec pour but de rassembler tous les logiciels de VoIP existants (Skype, TeamSpeak, Mumble, etc.) dans un seul logiciel. Le logiciel est d'abord utilisé par les joueurs, mais d'autres communautés se mettent rapidement à l'utiliser, comme les développeurs.

En mars 2020, Discord est utilisé en France, à l'initiative de certains enseignants et élèves, dans le cadre de la pandémie de Covid-19, par des établissements universitaires ou scolaires pour pallier les difficultés techniques des Espaces Numériques de Travail, saturés sur certaines plages horaires. Discord publie alors un guide sur son blog pour la création d'une classe virtuelle.

I. Créer un serveur Discord

Discord est basé sur un principe de serveurs. Chaque utilisateur peut fonder un ou plusieurs serveurs gratuitement et en devient dès lors l'administrateur. Selon les permissions du serveur, les utilisateurs peuvent rejoindre ou non les serveurs d'autres utilisateurs, grâce à des invitations. Sur leurs serveurs, les administrateurs peuvent créer des salons vocaux ou textuels et définir des permissions pour chaque utilisateur. Les permissions sont gérées sous forme de rôles.

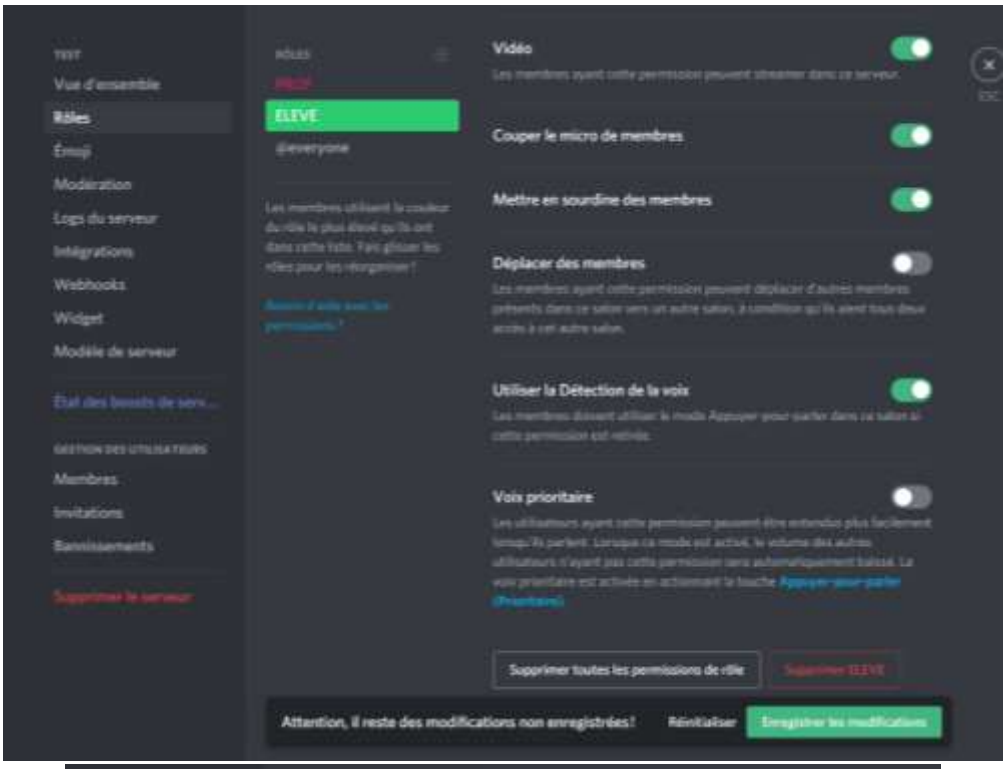
Outre la possibilité d'organiser des visioconférences, des réunions vocales. Discord permet également de chater, de partager des fichiers, de partager son écran et d'isoler des participants dans des groupes de travail autonomes. L'enseignant peut ainsi créer un salon général où il retrouve l'ensemble de ses élèves pour réaliser un webinaire par exemple. Il peut également répartir les élèves en groupes de travail autonomes et naviguer dans les différents groupes pour assister ses élèves.

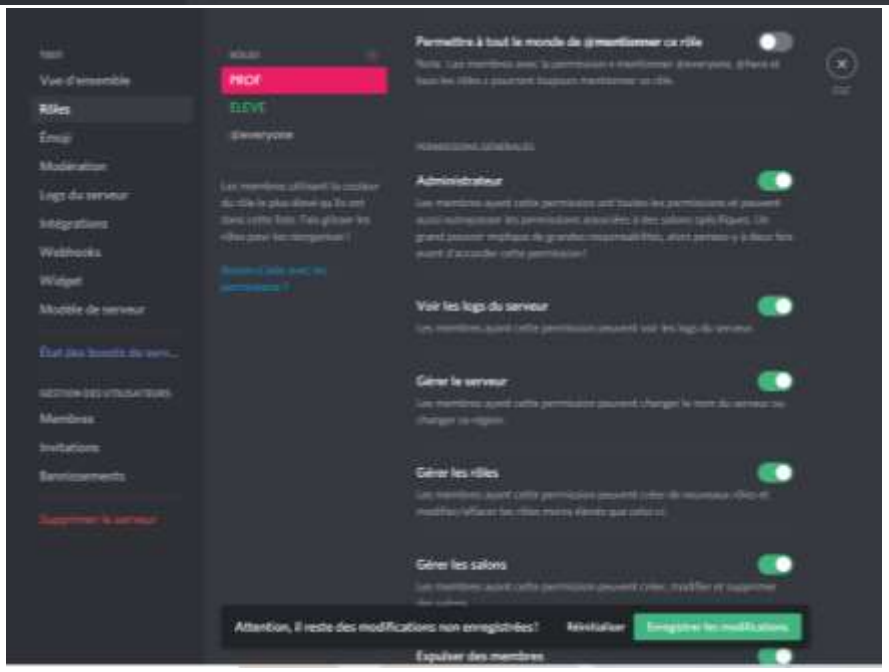
La procédure de création d'un serveur est simple. Il suffit de cliquer sur ajouter un serveur et d'en définir les paramètres et les rôles de ses membres. Plusieurs serveurs peuvent être créés en fonction du nombre de classe par exemple.
À titre d'exemple ci-dessous vous pouvez observer la création d'un serveur RH la création (réservé aux élèves de TSTMG RHC), d'un serveur C (CB serveur – le serveur PROF) et d'un serveur projet (C'FS pour le cas pratique). Vous constatez également qu'il y a 2 petites bulles, verte et rouge active. Il s'agit de bulles de discussion personnelle lancée à l'initiative d'un élève ou du professeur. Ces bulles de discussion permettent de dialoguer de manière isolée et sécurisée avec un élève ou un groupe d'élèves préalablement invités.


DISCORD
CBserver
NOUVELLES MENTIONS
SALONS VOCAUX
Général
TSTMG1 - DROIT
TSTMG3 - MANAGEME...
TSTMG - RHC
CG1-CEJM
LYCEE SAINT ANDRE
Ajouter un serveur


Oh, un autre serveur, hein ?
Crée un nouveau serveur et invite tes amis. C'est gratuit !
Rejoins un serveur avec un code ou un lien d'invitation.

Une fois le serveur créé, l'administrateur peut attribuer des rôles aux participants. Pour cela, vous devez cliquer sur les paramètres du serveur puis sur « rôle » et ajouter des rôles en cliquant (+). Ici vous constatez que 2 rôles ont été créés. Le rôle « prof » et le rôle « élève ». L'administrateur attribut des fonctionnalités à chacun des rôles. Il définit ainsi le champ d'action de chaque rôle en fonction des droits ouverts par l'administrateur.

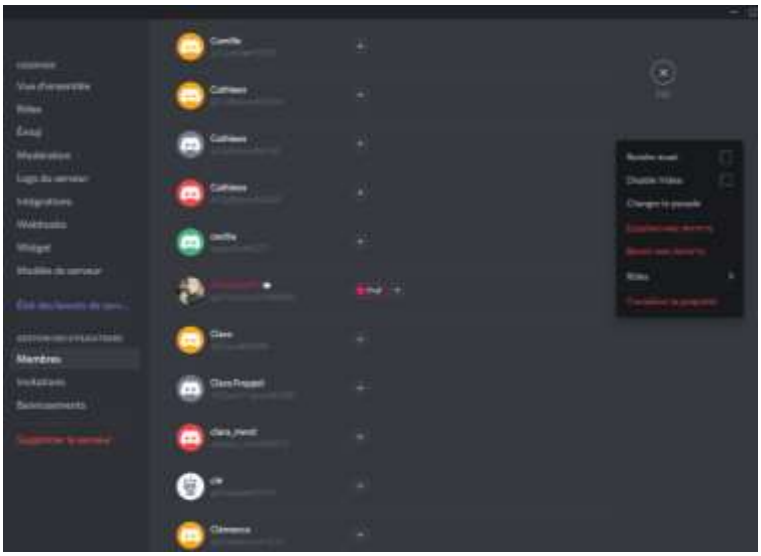


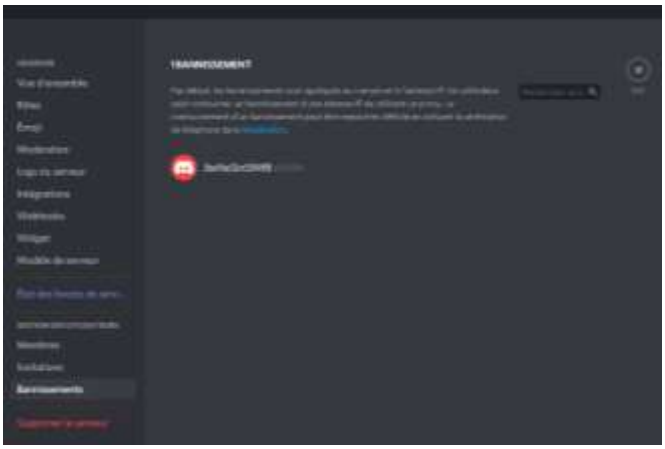


Une fois les rôles créés et les permissions attribuées, n'oubliez pas d'enregistrer.

A tout moment, vous pouvez vérifier les rôles attribués aux membres du serveur. Il est également possible, d'expulser un membre, de bannir définitivement un membre, de lui couper la parole, ou de modifier son pseudonyme. Pour ce faire, l'administrateur dois s'être attribué les droits lui permettant ses actions.

Par défaut, les membres du serveur sont limités en droit. Ils ne peuvent que participer aux discussions textuelles où vocales, partager des documents et participer à des réunions.



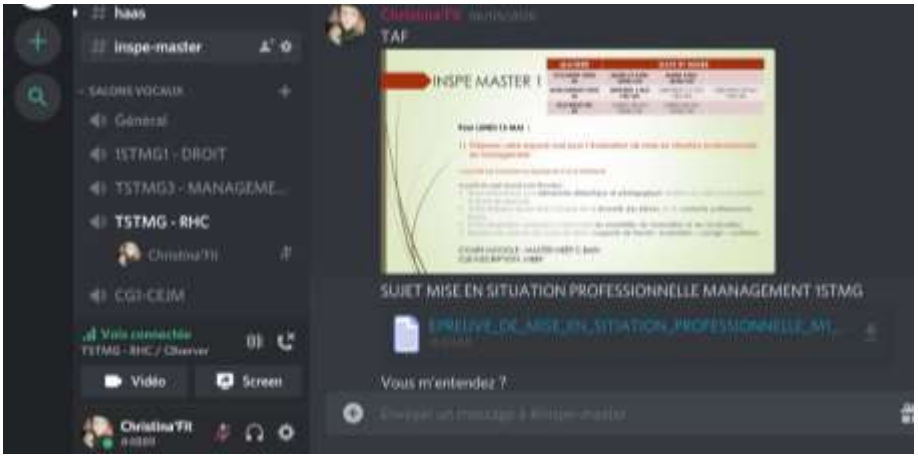


Attention !!! l'attribution des rôles est primordiale pour assurer la sécurité de votre serveur et des données qu'il contient.

L'administrateur « prof » doit avoir tous les droits car il pourra, limiter les accès, bannir et exclure des membres.

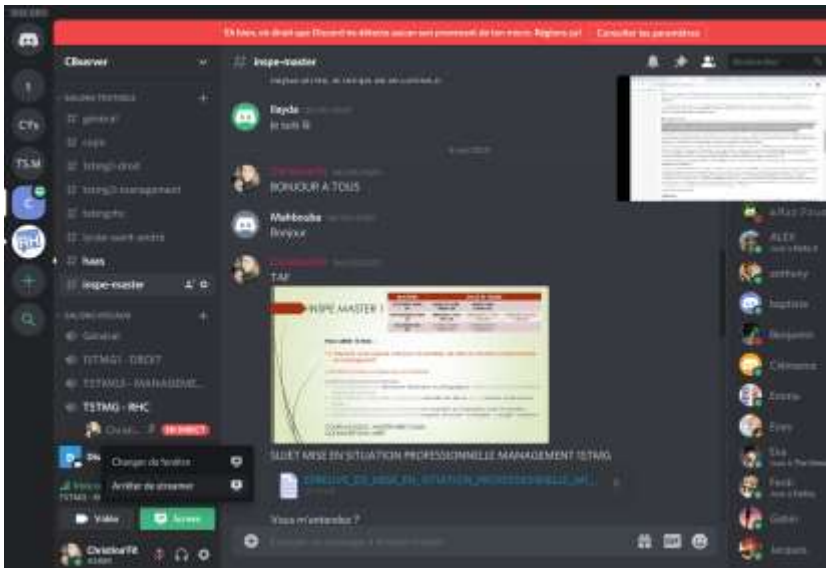
L'élève ou l'invité doit avoir le minimum de droit. Afin d'éviter toute faille de sécurité.

Ci-dessous vous pouvez constater, le partage d'un fichier textuel et d'un slide au format image.



Ici, il s'agit d'un partage d'écran, vu sur l'écran du professeur.

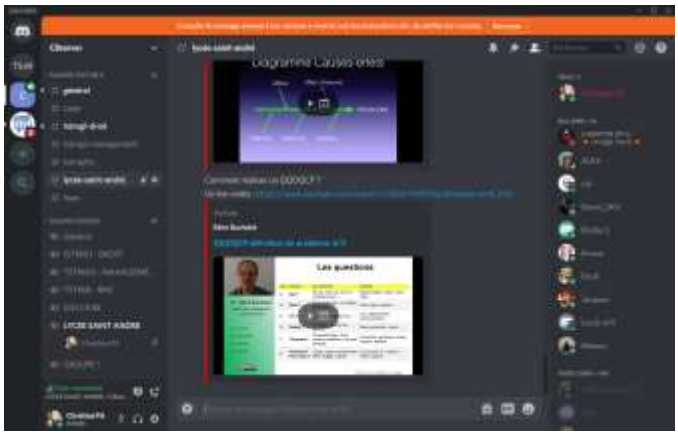
On constate également sur la navigation de droite que certains membres du serveur sont en train de jouer à des jeux en ligne. Fort heureusement, il n'était pas concerné par la classe en cours. Toutefois, cela pose un problème de confidentialité.



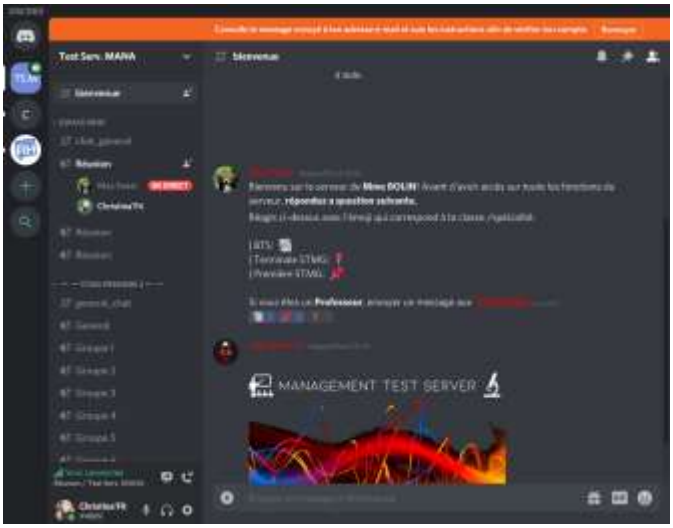
Ici il s'agit dans partage de url vers des vidéos Youtube.

On constate également dans la capture d'écran ci-dessous, dans la navigation de gauche, que le serveur comprend plusieurs salons textuels et plusieurs salons vocaux. L'administrateur a choisi de créer des salons par matière. Cette configuration est un choix de l'administrateur. Mais il autorise ainsi, aux membres du serveur d'accéder à tous les salons.

Pour éviter cela, il est possible de créer plusieurs serveurs et de limiter leur accès à des membre dédiés ou invités. Ou de créer des liens spécifiques dans le serveur textuel général, sur lesquels les élèves membres sont invités à cliquer pour accéder à des salons privés.



Pour les plus aguerris en informatique, il existe également une possibilité, via le langage de programmation (les Bots), de créer des liens de connexion privée. Pour autoriser l'accès au salon privé via le lien, il est possible de demander aux élèves membres de répondre à une question préalable. Si la réponse est juste, le lien d'accès au salon privé devient alors actif.



II. Les paramètres de sécurité de Discord

Discord permet de se protéger soi-même et son serveur (donc tous ses membres) via plusieurs fonctionnalités accessibles dans les paramètres de l'application et dans le panneau de configuration de son serveur.

Messages privés

Discord permet de choisir trois niveaux de protection face à la réception de messages privés et qui déterminent si Discord doit analyser les messages que vous recevez et supprimer les contenus explicites.

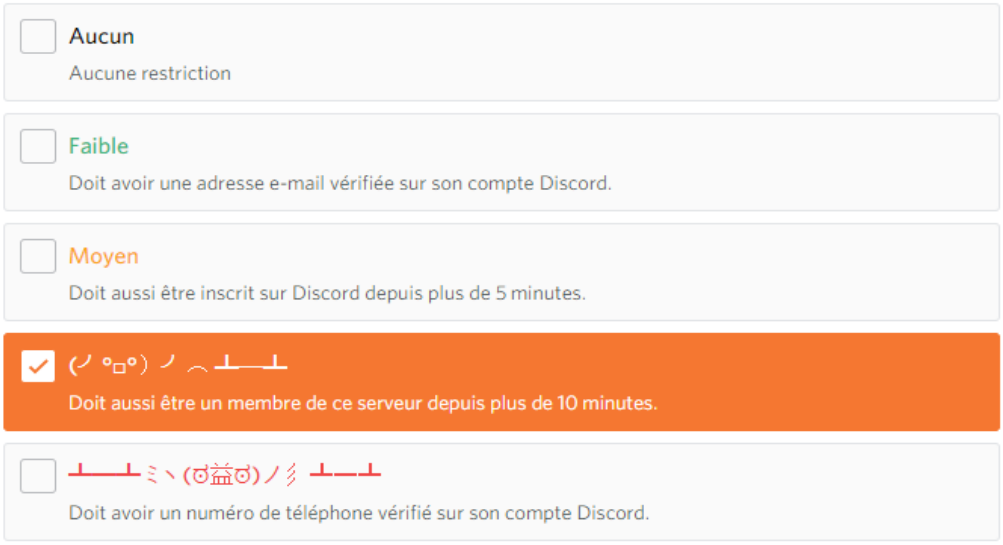
Attention ! ne divulguez aucune information personnelle.

Utilisez un pseudonyme. Ne donnez pas votre nom de famille.

Protéger son serveur

De la même façon que Discord le fait avec vos messages privés, l'application propose aux propriétaires d'un serveur de choisir entre trois niveaux de filtrage du contenu et supprime automatiquement les contenus présentant un caractère explicite (sexuels, violents, ..).

Discord propose également cinq niveaux de vérification des nouveaux arrivants du serveur et impose ainsi d'avoir une adresse mail et/ou un numéro de téléphone vérifié sur son compte pour envoyer des messages, ou encore d'être membre du serveur depuis plus de 10 minutes pour interagir avec les autres membres du serveur et accéder aux salons vocaux et écrits.



Attention, il est important d'inviter des membres par la création d'une URL différentes à chaque connexion. Ou d'inviter vos membres individuellement.
Cette action permet d'éviter les intrusions. Nous n'avons eu aucune intrusion en deux mois et demi d'utilisation.

Ne donnez pas votre numéro de téléphone.

Utilisez une adresse mail réservée à l'usage de Discord. Sans moyens d'identification de votre personne.

N'utilisez votre serveur qu'à des fins de cours. Ne jouez pas sur le même serveur.

Solutions extérieures

Discord donne la possibilité d'intégrer des « bots » à son serveur c'est-à-dire des « utilisateurs virtuels » qui sont des agents logiciel automatique ou semi-automatique et qui interagissent avec des serveurs informatiques. Ainsi, via le portail développeur de Discord, les utilisateurs peuvent ajouter des « bots » à leurs serveurs et les connecter à l'application. Nous allons voir que ces bots peuvent constituer une solution très efficace pour augmenter la sécurité de votre serveur et ajouter des fonctionnalités pratiques à celui-ci.

Utilisons le cas du bot « Raid Protect », ce « bot » permet de protéger un serveur d'un raid, c'est-à-dire d'une arrivée massive d'utilisateurs dont le but est de saturer le serveur et ses canaux de discussions.
Pour ce faire, le bot utilise un système « d'anti-spam ». Cela signifie que le bot est capable de reconnaître une action où un utilisateur qui envoie à répétitions des messages dont le but est de saturer le salon. Il est alors possible de bannir automatiquement celui-ci.

Ensuite, de la même façon que sur certain site internet, ce bot met en place des codes Captcha que les utilisateurs doivent compléter à leur arrivée sur le serveur, cela permet de s'assurer que l'utilisateur n'est pas un robot et le cas échéant de l'empêcher d'accéder aux contenus du serveurs dont, les salons vocaux et écrits.

Les bots, sont donc une façon de protéger son serveur à la condition de prendre le temps de les configurer (une fois le bot ajouté, vous devez le configurer pour votre serveur). Par ailleurs, il existe de nombreux « bots » qui ajoutent chacun leur lot de fonctionnalités, ne se limitant pas à la sécurité mais permettant d'ajouter des messages personnalisés et ou compteurs de membres, les possibilités sont infinies…

… Attention, il est préférable de créer votre propre Bot. En effet, les bots téléchargeables ne garantissent pas le risque de programmes malveillants.

Comme de nombreuses solutions (Skype, Zoom…). Discord n'est pas à l'abris de cyberattaques. Installez préalablement des antispam et des antivirus sur votre pc.

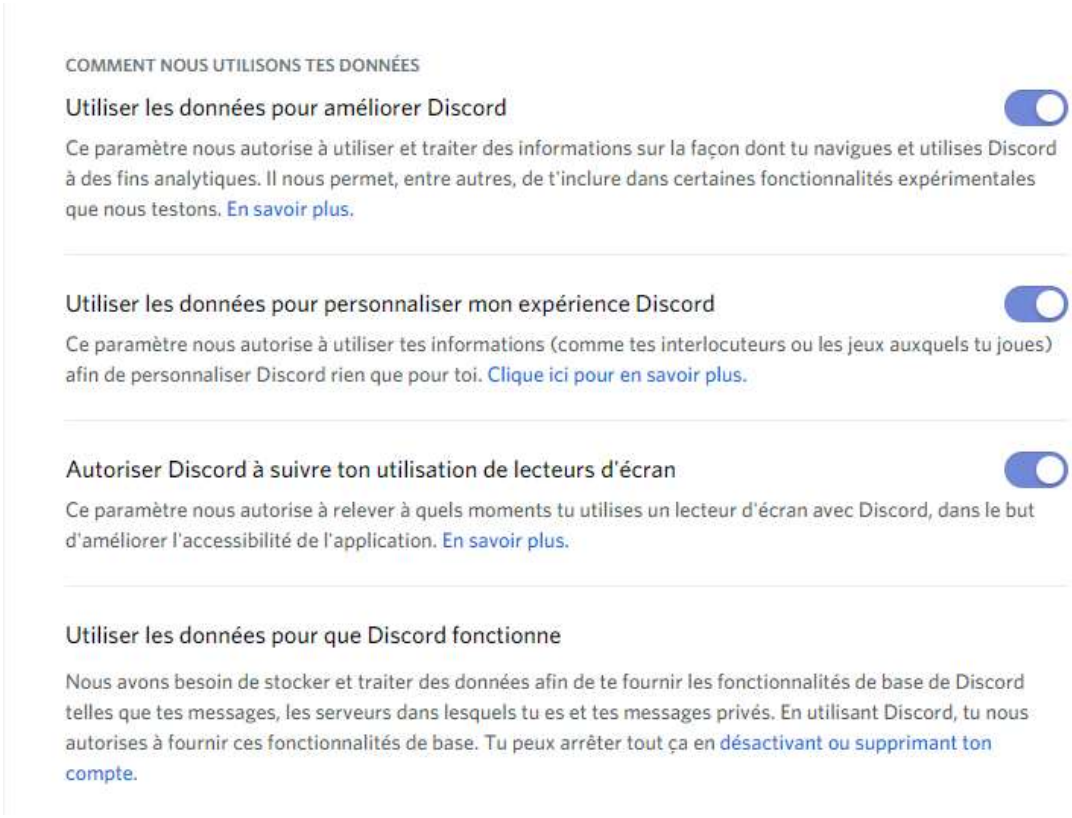
De même, Discord a déclenché la controverse, en refusant de diffuser son code source. D'où, la réaction de certains professionnels du métier de laisser croire que Discord est un Spyware. Cependant, en agissant ainsi Discord souhaitait éviter de dévoiler d'éventuelles failles de sécurité, facilement accessibles après diffusion du code source. Il reste malgré tout difficile de vérifier l'intégrité et la fiabilité du service proposé par Discord.

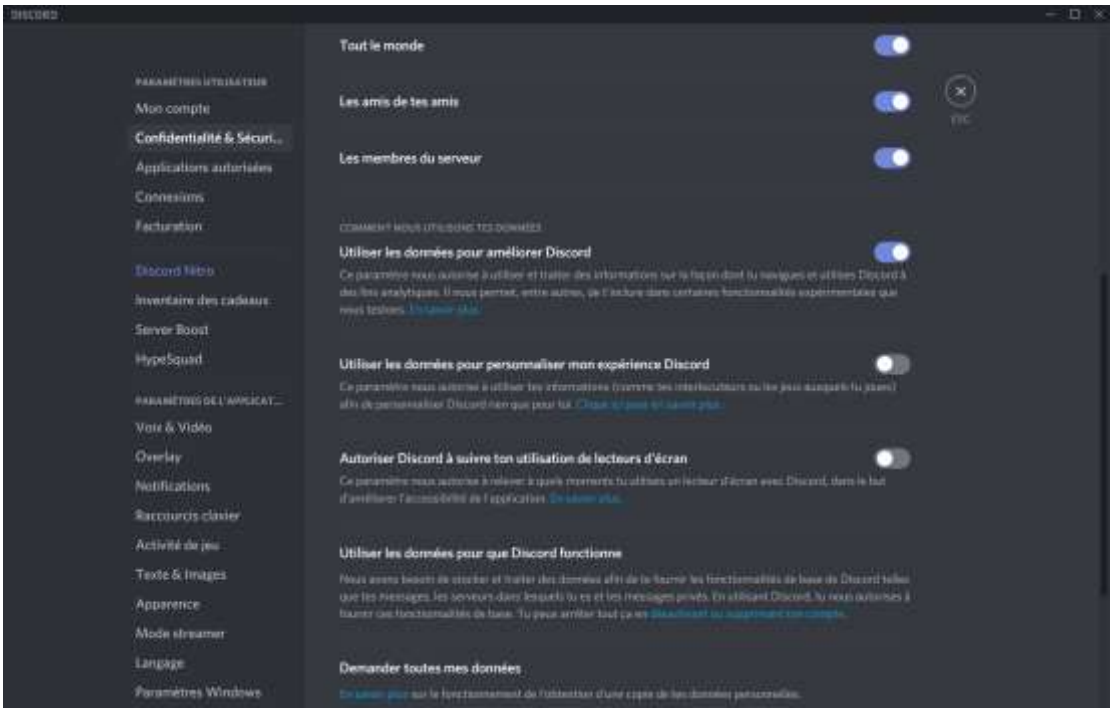
Il est donc important de vérifier les sources d'information et d'utiliser ses solutions avec précautions.

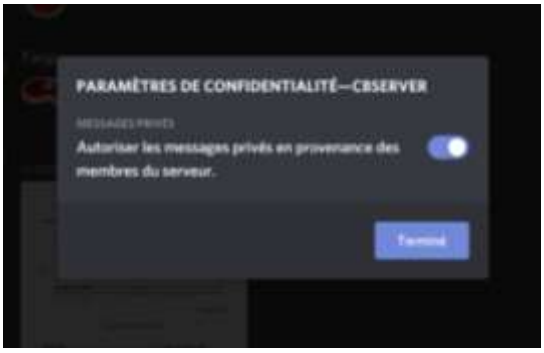
III. Protéger ses données personnelles

Comme la plupart des applications gratuites (et réseaux sociaux), Discord récolte des données sur ses utilisateurs, la façon dont ceux-ci utilisent discord, comment vous naviguez dans l'application, à quelle fréquence vous l'utilisez, les messages que vous envoyez et les serveurs que vous rejoignez … Ces données sont utilisées par Discord pour améliorer l'application à des fins commerciales.

Il est possible de désactiver les différents processus que discord utilise pour collecter vos données, en accédant aux paramètres de confidentialités de l'applications.







Il est intéressant de constater que Discord collecte des données sur les applications que nous exécutons sur nos appareils. Cela s'explique principalement par le fait que Discord a d'abord été conçu pour les joueurs et permet ainsi de lancer ces jeux directement aux travers de Discord.

Cependant, il semblerait que Discord se serve aussi de ces données à des fins commerciales, par exemple pour déterminer quel logiciels l'utilisateur serait susceptible d'acheter dans le futur.

Enfin, vous pouvez demander à discord de vous envoyer toutes les données récoltées sur votre compte et vous recevrez, sous trente jours, un lien vers un fichier contenant vos données. Ce qui inclut, votre compte (Adresse IP, compte reliés, session, paramètres utilisateurs, ..), vos messages (Privés, Serveurs, Groupes, ..), les programmes que vous exécutez sur votre ordinateur (Jeux, logiciels, ..).

Attention ! Pensez à décocher les autorisations demandées par Discord concernant la possibilité de récolter des données personnelles.

En effet, la plateforme est gratuite, et elle est gérée par une petite entreprise. Qui a certainement profité de l'usage de données personnelles.
La solution Discord stocke, en effet, des éléments relevant des conversations.
Elle tend aujourd'hui à jouer la transparence, du fait que les usages ne sont plus réservés aux gamers et tendent à se généraliser dans le domaine de l'éduction et de l'entreprise.
D'autant que Zoom a été montré du doigt pendant la crise du covid 19 à cause de nombreuses failles de sécurité. Zoom a été déconseillé, voir même interdit dans certains états aux USA.

Pour conclure, il est important de dire que Discord est une excellente application. Parfaitement adaptée à un usage pédagogique. Toutefois, comme toute solution numérique, elle nécessite un usage réfléchi et sécurisé, car elle n'est pas à l'abri de cyberattaque.

Concernant la RGPD, l'organisation Discord a nettement amélioré sa mise en conformité. Le processus n'est certes pas encore parfait et reste non conforme. Cependant, la pression des utilisateurs pousse la direction de Discord à plus de transparence et à la mise en conformité. Il s'est laissé entendre sur la toile, de l'éventualité d'une version payante afin de permettre à Discord de continuer à se développer et répondre aux besoins des professionnels.

Pour ma part, après deux mois et demi d'utilisation, nous n'avons eu aucune intrusion, et aucune attaque. Nos données sont restées centrées sur les séances de cours. Donc rien de personnel, ou relevant de la vie privée, à part nos adresses IP et nos cours. WhatsApp est depuis peu chiffré bout à bout.
Tout comme WhatsApp qui a également été très sollicité par les enseignants.
Les accès étaient très fluides et rapides (pas de problème de connexion). Aucune publicité ou campagne de @mailing. La plateforme a évolué en proposant, au bout de quatre semaines d'utilisation, la visioconférence.
Aucun virus ou spam n'a été détecté sur mon pc, j'effectuais régulièrement des vérifications.