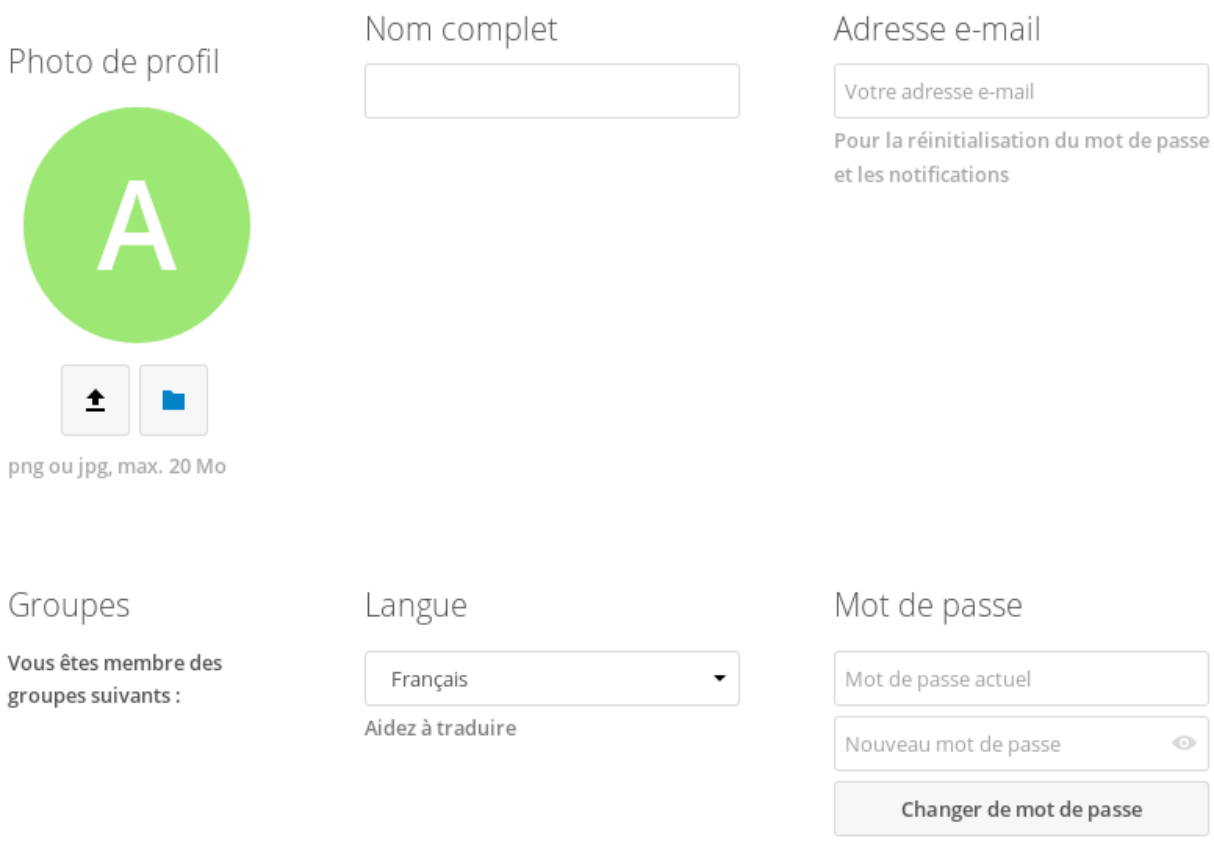
DÉMARRAGE RAPIDE DE GIBBERFISH

Bienvenue sur Gibberfish ! Notre objectif est votre vie privée et la sécurité, mais nous avons besoin que vous soyez un participant égal. Voici quelques suggestions pour vous aider à démarrer.

PROFIL

Si c'est votre première fois vous connecter, vous devez prendre quelques minutes pour remplir votre profil et Pendant que vous y êtes, changez votre mot de passe! Cliquez sur ⚙ l'en haut à droite d'angle et choisissez **Personal** pour modifier votre profil.



PHRASES CLÉS

Une bonne phrase est extrêmement importante pour la sauvegarde de vos données. Nous et nombreux experts de la sécurité est recommandé de créer des mots de passe en utilisant la méthode Diceware. Il sagit de **la seule méthode** de génération de mot de passe que nous estimons sécurisés. Son facile à faire et il fournit des passphrases ultra résistantes qui peut vaincre même les adversaires les plus débrouillards.

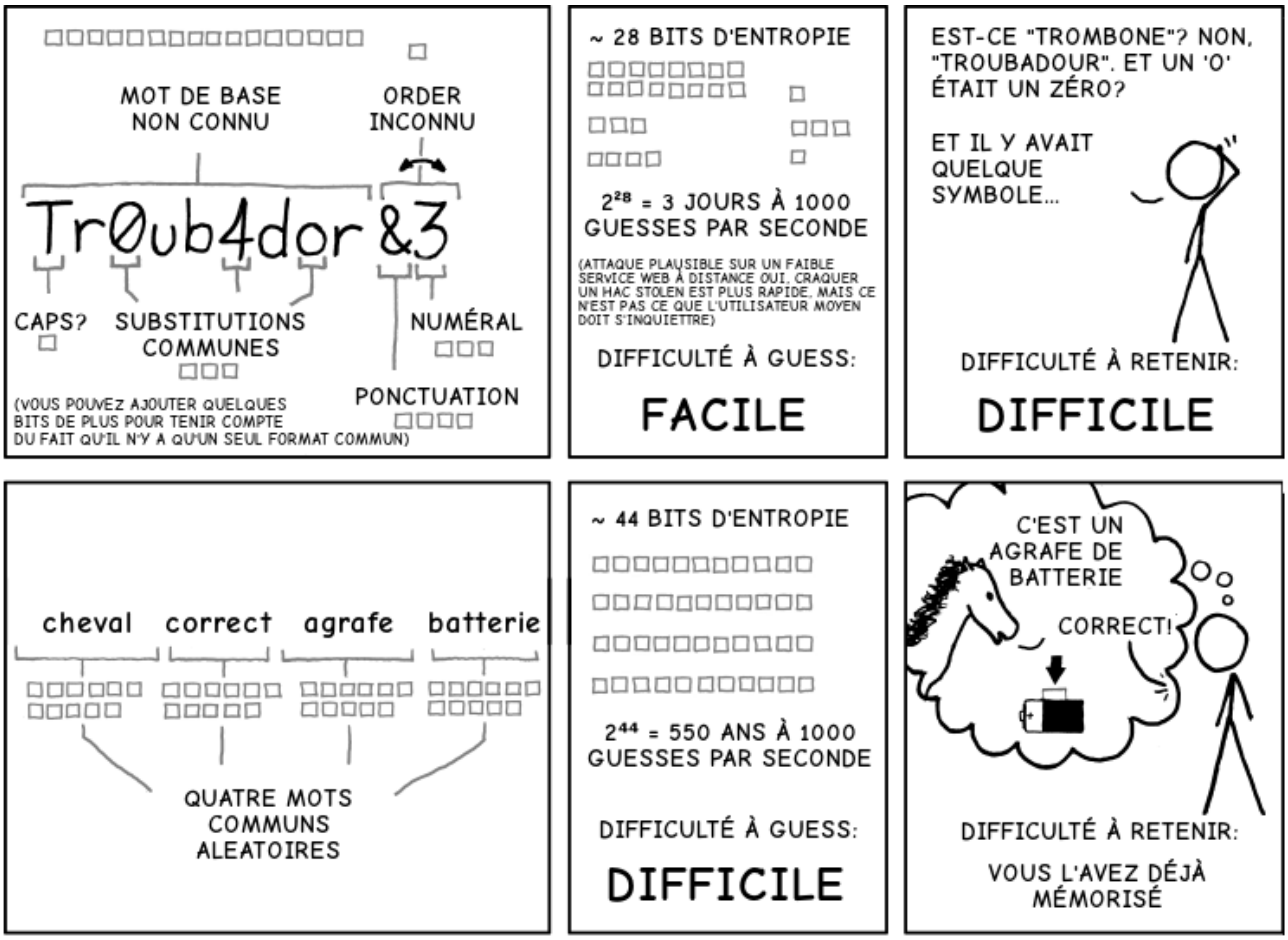


image avec autorisation de xkcd.com.

Alors que la bande dessinée cidessus explique le concept la méthode Diceware recommande une longueur de mot de passe de **5 ou plusieurs mots** pour une sécurité optimale.

Ne jamais utiliser un mot de passe pour votre login Gibberfish que vous utilisez nimporte où ailleurs.

Toujours générer un mot de passe unique pour tout service le compte ou le périphérique.

AUTHENTIFICATION À DEUX FACTEURS

Une fois que vous avez changé votre mot de passe, nous encourageons fortement d'activer l'authentification à deux facteurs (« 2FA »). Il s'agit d'installer une application sur votre appareil mobile qui génère un code à 6 chiffres unique, que vous devez entrer chaque fois que vous ouvrez une session. Quelqu'un pirater votre compte, ils auraient besoin de connaître votre mot de passe et posséder physiquement votre téléphone. Cette combinaison vous tient plus sûr. Parce que Gibberfish fait partie de l'écosystème de la Nextcloud, vous pouvez utiliser le Nextcloud 2FA app. Cette application prend en charge FreeOTP, qui peut être téléchargée dans l'app store pour les appareils Android et iOS.

CLÉS DE VOÛTES

Si vous nêtes pas déjà lhabitude de le faire il serait une bonne idée pour stocker vos mots de passe dans un caveau clé comme KeePass. Voûtes clés le rendent facile à retenir solidement tous vos mots de passe. Vous aurez besoin de verrouiller votre voûte clé luimême dun mot de passe Diceware générée. En outre nous vous recommandons **fortement** de que vous activez le chiffrement complet des disques sur le périphérique de stocker votre clé vault.

En utilisant cette méthode assure vous navez quà retenir un mot de passe celui de déverrouiller votre clé vault.

HYGIÈNE DIGITAL

Bonne hygiène digital est une utilisation uniforme des pratiques de sécurité robuste.

Nous entendons par “robuste” les procédures qui ont été mis en place ou contrôlés par des experts de la sécurité de confiance. Ceuxci incluent mais ne se limitent pas à le projet de l’Electronic Frontier Foundation (EFF) le projet Guardian et Tor.

Nous utilisons “uniforme” à souligner que l’utilisation intermittente de toute pratique de sécurité est aussi mauvaise qu’on utilise ne pas du tout. Une fois que vous développez un modèle de menace et d’une stratégie pour vaincre, vous devez appliquer cette stratégie, chaque fois que vous vous livrez à des activités privées.

MENACES

Comprendre les menaces de votre groupe et vous rencontrerez est une étape importante dans létablissement dune stratégie de sécurité utile. Lobjectif est dutiliser seulement les techniques nécessaires à la protection contre vos adversaires susceptibles. Cela empêchera votre régime de sécurité deviennent tellement lourde que vous cessez de lutiliser. Votre administrateur peut avoir déjà créé un modèle de menace décrivant les défis sécuritaires que vous et votre groupe peuvent sattendre. Si vous nêtes pas sûr veuillez les contacter et demander.

Chaque utilisateur doit comprendre le modèle de menace de votre groupe et utiliser systématiquement les mêmes pratiques de sécurité.

Pour plus dinformations sur les modèles de menace veuillez vous référer à cette excellente introduction produite par l’EFF.

COMMUNICATIONS EXISTANTES

Il est probable que vous ajoutez Gibberfish à une variété de comptes existants et des services associés à vos activités en ligne. Ces services et les comptes plus anciens peuvent déjà être compromises. Nous recommandons lutilisation des comptes de frais pour toute activité qui implique votre serveur Gibberfish le contenu qui y sont stockées ou les activités qui lui sont associées.

Nous reconnaissons que ce nest pas toujours commode ou le plus approprié pour chaque utilisateur. Dans ce cas veuillez prendre le temps de refixer tout compte ou le service que vous voulez utiliser pour les activités privées. Changer vos mots de passe afin de bloquer sans autorisation dutilisateurs qui peuvent avoir accédé à votre insu. Dans la mesure du possible activer lautorisation de deux facteurs. Recherchez les mises à jour logicielles pour tous vos appareils y compris votre téléphone et installezles.

TOR

Lutilisation de Tor est le seul meilleur moyen pour protéger votre vie privée en ligne. Cest pourquoi nous utilisent Tor pour déployer votre serveur Gibberfish. Alors quil se réfère spécifiquement au projet **T**he **O**nion **R**outer, Tor est venu pour inclure une variété de produits gratuits et services participants pourront utiliser pour protéger leurs activités en ligne. Nous recommandons que tout le monde utiliser le Pack de navigation Tor pour aider à anonymiser leur présence en ligne.

Veuillez lire attentivement la documentation et la FAQ que Tor fournit sur la navigation sur leur réseau. Ils ont des recommandations importantes pour préserver votre vie privée. Ce qui est important, en utilisant le Pack de navigation Tor ne garantit pas que toutes vos activités en ligne sont anonymes.

Car votre sécurité doit dégénérer Tor a autres outils gratuits pour aider. Lorsque vous évaluez votre modèle de menace vous pouvez enquêter sur les serveurs de passerelle et les queues. Serveurs de passerelle aux gens de Tor dans les pays qui bloque laccès. Uni/bilatéral est un système dexploitation Linux avec les programmes couramment utilisés tous sur une clé USB. Il permet de calcul extrêmement privé.

Découvrez ces activités et autres services Tor à
https://www.torproject.org/projects/projects.html.en

APPELS VIDÉO

L’application “Talk” de Nextcloud permet de créer et de rejoindre les appels vidéo dans votre navigateur web. Pour des performances optimales sur les appareils mobiles nous recommandons que vous installez et utilisez lapplication mobile “Nextcloud Talk” disponible sur iTunes, Google Play et F-Droid.

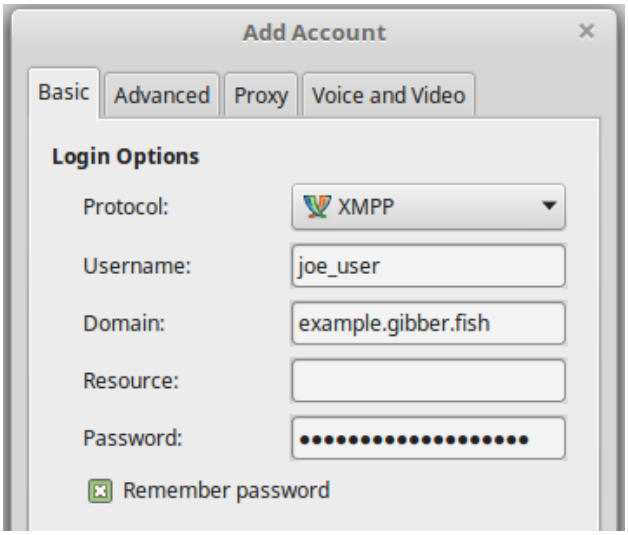
CHAT

Le système de chat utilise le protocole standard XMPP, qui vous permettra de discuter non seulement avec d'autres utilisateurs de Gibberfish, mais aussi avec une autre personne dans le monde en utilisant un serveur XMPP. Votre adresse XMPP est <votre nom d'utilisateur> @<votre serveur gibberfish>. Par exemple,

joe_user@example.gibber.fish

Lors de votre première connexion votre liste de chat sur le côté droit de lécran sera vide. Dans le menu en bas vous pouvez **ajouter un Contact**. Commencez simplement à taper et il recherchera automatiquement pour les utilisateurs existants sur le serveur ou vous pouvez taper ladresse XMPP des utilisateurs externes.

Pour rester connecté lorsque vous nêtes pas connecté à Gibberfish vous pouvez aussi connecter au serveur en utilisant directement un client XMPPcompatible comme Adium Pidgin ou une des nombreuses applications mobiles.



Le serveur de chat est également accessible comme un Tor "service d'oignon" sur le port 5222. Demandez à votre administrateur pour l'adresse de votre serveur Tor.

Toutefois, lorsque le chat avec les utilisateurs en dehors de votre serveur, vous n'avez aucune garantie de protection des renseignements personnels à moins que vous **et** vos contacts utilisent un plugin de chiffrement bout à bout comme « OTR ». La plupart des clients de chat supporte le cryptage de bout à bout et ont des guides pour vous aider à comprendre et à lui permettre.

CLIENTS DE BUREAU ET MOBILES

Gibberfish fonctionne avec le Nextcloud les clients de bureau et mobiles pour vous permettre de synchroniser automatiquement les fichiers vers et depuis le serveur. Par mesure de sécurité cest désactivé par défaut. Si vous souhaitez utiliser ces clients demandez à votre administrateur de modifier les règles daccès de fichier. Si vous décidez de synchronisation de fichiers localement ne faire que si vous avez activé le chiffrement complet des disques pour votre appareil. Cela protège vos fichiers si votre appareil est perdu volé ou hacké.

Il est difficile, mais possible, pour vos données d'être interceptées par des adversaires ingénieux lors du transport. Pour cette raison, nous **ne recommandons pas** la synchronisation de vos données sans considérer soigneusement votre modèle de menaces et de vos pratiques de sécurité.

DAVANTAGE DE LECTURE

Pour une documentation plus complète les fonctionnalités de base, veuillez vous référer au manuel d'utilisation Nextcloud, qui est aussi situé dans votre dossier Gibberfish.

Administrateurs devraient également se familiariser avec le manuel de l'Admin.

Enfin nous recommandons de vous abonner au Gibberfish Blog dans lapplication de nouvelles pour tenir à jour sur les annonces importantes et notre déclaration de canaris.

DERNIÈRES NOTES

Nous espérons que vous apprécierez à laide de Gibberfish. Nous avons travaillé dur make it un sûr et facileà utiliser la plateforme comme les autres contributeurs indépendants aux divers projets open source que nous avons intégré dans notre service. Remerciement spécial aux gens de Nextcloud sans lesquels notre plateforme ne serait pas possible.

Nous comptons sur les dons pour survivre. Si vous pouvez vous le permettre sil vous plaît envisager de faire une contribution charitable de tout montant à https//gibberfish.org/fr/donate. On lappréciera énormément. Merci!

Pour des raisons de sécurité nous avons seulement répondre aux demandes auprès de votre administrateur inscrit. Si vous avez des questions liées au service sil vous plaît demandez à votre administrateur.