Les points clés de SQRL

Table des matières

Oui, mais… et si ?

Les trois règles d'or de SQRL

Introduction à la version française

Ce document se veut être la traduction la plus fidèle possible des pages "SQRL Essentials" rédigées en anglais par Steve Gibson et accessibles ici : https://sqrl.grc.com/pages/what_is_sqrl/. Les éventuelles erreurs (fautes de frappe ou incompréhensions) sont de mon fait uniquement et ne peuvent en aucun cas être reprochées à Steve Gibson. Si vous trouvez des erreurs, ou si vous souhaitez apporter des modifications et améliorations, merci de le signaler sur le forum, dans le fil de discussion dédiée à la version française de SQRL. Merci et bonne lecture ! SQRL va changer le monde et il n'y a pas de raison qu'il ne le fasse pas en français aussi !

Fabrice Neuman

Comprendre SQRL

Cette page explique ce que fait SQRL et pourquoi nous sommes persuadés que ce système va changer le monde.

SQRL se connecte pour vous à vos services en ligne

Plutôt que d'utiliser un identifiant (un pseudo ou un email/courriel) et un mot de passe, SQRL utilise une application pour vous authentifier auprès des sites Web compatibles.

Lorsque SQRL vous authentifie auprès d'un site Web, votre identité est représentée par une longue suite de caractères ressemblant à ça : E6Qs2gX7W-Pwi9Y3Kam-kuYjLSWXCt-yBcymWl-HAuo.

Votre identité SQRL, cette longue suite de caractères donc, est différente pour chacun des sites Web auquel vous vous connectez. Mais elle reste inchangée lorsque vous retournez sur un site auquel vous vous êtes déjà connecté au moins une fois à l'aide de SQRL. Cela signifie que les sites Web ne savent jamais qui vous êtes, mais ils savent pourtant quand vous revenez.

Vous pouvez donc choisir de rester anonyme et donc de ne jamais donner votre véritable nom à un site Web, par exemple pour publier un commentaire à un article de blog. SQRL ne vous identifie jamais par autre chose que par cette longue suite de caractères.

Pour les autres sites Web auprès desquels vous souhaitez être reconnu par **votre véritable nom**, par exemple Amazon, Facebook, Netflix ou votre banque, vous devrez vous-même associer votre nom au code unique créé par SQRL pour chacun d'eux. C'est une des fonctions intégrées à SQRL.

SQRL a demandé 5 ans de développement. Il est maintenant finalisé et les pages et articles de ce forum SQRL ont été conçus pour que vous puissiez facilement tout savoir au sujet de ce système.

Vous y trouverez les différentes versions des applications SQRL qui vous permettront de découvrir comment vous connecter aux sites Web compatibles avec SQRL, qui sont de plus en plus nombreux. Nous sommes persuadés que SQRL est l'avenir des méthodes d'authentification et de vérification d'identité des sites Web. Et nous espérons que vous le serez aussi.

Pour aller plus loin, nous vous suggérons de poursuivre par la lecture de la section suivante, intitulée Questions/Réponses d'Introduction.

Questions/Réponses d'Introduction

Cette courte collection de questions/réponses présente à ceux qui ne les connaissent pas encore les principaux concepts, fonctions et bénéfices de SQRL.

Quels sont les principes fondamentaux de SQRL ?

1. Les utilisateurs de SQRL doivent utiliser une application SQRL sur tous leurs appareils. Il en existe des versions gratuites pour tous les modèles.
2. Lorsque l'on utilise une application SQRL, une identité principale est créée et partagée entre tous les appareils. Les sites Web compatibles SQRL lancent automatiquement l'application pour permettre à l'utilisateur de s'identifier de manière sécurisée.
3. Les identités SQRL sont anonymes et SQRL fournit des identités différentes et uniques et anonymes pour chaque site Web. Autrement dit, les identités SQRL ne peuvent pas être utilisées pour vous suivre à la trace sur Internet.

- SQRL est gratuit et le restera toujours.
- SQRL est ouvert et distribuable. Tout le monde peut l'utiliser, créer des applications de connexion et ainsi créer des sites Web plus sûrs.
- SQRL est sécurisé. Les sites Web n'ayant plus de secret à conserver, cela n'a aucune importance s'ils se font pirater. L'identité de l'utilisateur est protégée quelles que soient les circonstances.
- SQRL remplace les identifiants, les courriels, les mots de passe, les codes d'authentification et tout le reste. Une fois que vous vous êtes fait reconnaître par un site Web à l'aide de votre identité SQRL, SQRL est l'unique moyen d'authentification dont vous aurez jamais besoin… et sans besoin non plus de vous souvenir de quoi que ce soit.

Comment SQRL protège ses utilisateurs en cas de piratage des sites Web qui l'utilisent ?

Les sites Web ont besoin de pouvoir s'assurer de l'identité d'un visiteur. Avec SQRL, c'est la seule chose qu'un site Web est capable de faire. Lorsqu'ils s'appuient sur le système archaïque des mots de passe, les sites Web se voient dans l'obligation de conserver ces mots de passe à l'abri des regards. SQRL, à l'inverse, ne confie aucun secret à garder aux sites Web. Du coup, même si le site Web se fait pirater, pas de problème. Grâce à SQRL, les sites Web n'ont littéralement rien à perdre !

Je croyais que SQRL éliminait les mots de passe… mais SQRL a un mot de passe ?

Oui… ou votre empreinte digitale, ou votre visage, ou tout ce que vous voulez. Et c'est uniquement pour vous assurer que personne d'autre que vous n'utilise votre application SQRL sans votre permission. SQRL se connecte pour vous et en tant que vous. Il va sans dire donc qu'il vaut mieux que vous soyez le/la seul(e) à pouvoir utiliser l'application SQRL. C'est la raison pour laquelle l'accès à SQRL est protégé par un mot de passe que vous êtes le/la seul(e) à connaître. Si votre appareil propose un mécanisme de sécurisation biométrique (empreinte digitale, reconnaissance faciale, empreinte vocale ou autre chose), vous pouvez alors l'utiliser à la place du mot de passe. Nous voulons juste nous assurer que personne ne peut utiliser votre application SQRL à votre insu.

Et n'oubliez pas que dans un monde idéal où SQRL serait utilisé partout, vous n'avez qu'un unique mot de passe à retenir : celui qui vous permet de déverrouiller SQRL. Et vous n'aurez jamais besoin de le changer, à moins que vous en ayez envie. Même si un site Web se fait pirater, pas de besoin de changer de mot de passe puisque vous ne lui en avez jamais confié aucun.

J'ai entendu que SQRL était une solution à 2 parties. Qu'est-ce que ça signifie ?

Cela signifie que c'est une solution qui se passe de tout intermédiaire. Il n'y a que vous et le site Web. Avec SQRL, vous n'avez besoin de faire confiance à personne d'autre. Personne qui ait besoin de prendre des précautions. Personne qui puisse se faire pirater. Aucune personne appartenant à un quelconque gouvernement pouvant vous forcer à révéler votre identité. Et les sites Web n'ont aucun moyen de révéler qui vous êtes à partir de votre identité SQRL puisque cette dernière n'est constituée que d'une longue suite de caractères aléatoires, différente pour chaque site Web. Autrement dit, les sites Web n'ont aucun moyen de comparer votre identité SQRL entre eux.

Cela semble trop beau pour être vrai. Comment se fait-il que cela n'ait pas été fait avant ?

La création d'un système complet, sécurisé et fiable requiert l'assemblage précis d'un grand nombre d'éléments disparates. Et plusieurs de ces éléments n'existaient pas auparavant. Cela a demandé cinq ans de travail. Sans aucune motivation financière. Et il ne peut pas y en avoir.

Parce qu'un système d'authentification sur Internet vraiment révolutionnaire, puisqu'il élimine le besoin d'identifiants et de mots de passe, doit être utilisable gratuitement par tout le monde. Les seuls bénéficiaires ne peuvent être que les utilisateurs de SQRL et les sites Web qui désormais peuvent s'authentifier entre eux de manière fiable et sécurisée. De nombreuses entreprises ont créé des solutions privées et propriétaires basées sur la simple règle du « faites-nous confiance ». Avec la volonté de vendre leur solution. Mais cette problématique est bien trop vitale pour la laisser entre les mains d'un seul propriétaire. La solution devait absolument être gratuite pour qu'elle puisse être la propriété de tous. C'est maintenant le cas.

Et maintenant ?

Lisez la page suivante: « Bien commencer avec SQRL ». Sur la page correspondante en anglais (http://sqrl.grc.com/pages/getting_started_with_sqrl/), deux vidéos vous permettent de découvrir le fonctionnement de SQRL, de télécharger des applis SQRL, de créer votre identité SQRL et de l'utiliser pour vous connecter à quelques sites ! Les mêmes liens sont disponibles dans cette traduction française.

Merci de l'intérêt que vous portez à SQRL. Vous êtes convaincu et enthousiaste ? Parlez-en autour de vous. Demandez aux sites Web que vous utilisez de devenir compatibles avec SQRL afin que vous puissiez vous débarrasser de vos archaïques mots de passe, gestionnaires de mots de passe, solutions d'authentification à deux facteurs basées sur la génération de codes à usage unique et de tous ces autres pansements auxquels nous nous sommes trop habitués par nécessité !

Bien démarrer avec SQRL

Vous débutez avec SQRL? Cette page est là pour vous aider à bien commencer.

SQRL: Le Guide du débutant

Vous n'avez encore jamais utilisé SQRL mais vous aimeriez savoir comment ? Vous êtes au bon endroit !

Commencer avec SQRL, c'est aussi facile que de compter jusqu'à 3…

1. Récupérez une application SQRL pour Android, iOS, Windows, Chrome ou Firefox.
2. Créez l'identité SQRL que vous utiliserez probablement pendant toute votre vie.
3. Utilisez votre application SQRL pour vous authentifier sur tous les sites compatibles.

Faites-vous une idée de la façon de fonctionner de SQRL en le voyant à l'œuvre ! Les vidéos suivantes, créées par des utilisateurs, devraient vous aider à mieux comprendre l'expérience d'utilisation de SQRL, pour que vous sachiez à quoi vous attendre:

Faites-vous une idée du fonctionnement de SQRL grâce aux deux vidéos (en anglais) disponibles sur cette page (https://sqrl.grc.com/threads/a-video-demonstrating-sqrl.293/).

Où puis-je obtenir une application SQRL?

Des applications SQRL sont en cours de développement pour tous les systèmes d'exploitation et tous les appareils :

- *SQRL pour Windows* par Steve Gibson (GRC)
  (Télécharger ici - https://www.grc.com/files/sqrl.exe).
  Si vous utilisez un PC Windows, nous vous conseillons vivement de commencer par utiliser l'application SQRL de GRC. Elle dispose de la totalité des fonctions et propose un grand nombre d'explications pas à pas pour aider tous les nouveaux utilisateurs à comprendre facilement son fonctionnement. Une fois que vous l'aurez utilisée pour créer votre identité SQRL, vous pourrez exporter cette dernière vers n'importe quelle autre application SQRL.

Les applications de Daniel, Jeff et Jaap pour Android, iOS, Firefox et Chrome sont en cours de développement et avancent rapidement. Elles sont fonctionnelles mais pour l'instant moins avancées que l'application SQRL pour Windows de GRC. Il leur manque encore quelques fonctions critiques. Mais si vous êtes tentés… n'hésitez pas… et vous pourrez ensuite participer en nous faisant part de votre expérience ! :

- *SQRL pour Android* par Daniel Persson
  (Google Play Store - https://play.google.com/store/apps/details?id=org.ea.sqrl)
- *SQRL pour iOS* par Jeff Arthur
  (Obtenir pour iOS - http://eepurl.com/bfmQ3z)
- *SQRL* - Extension pour Firefox et Chrome par Jaap
  (sur Github - https://github.com/Jaaap/SQRL)

OK, j'ai installé l'application SQRL et créé mon identité, qu'est-ce que je fais maintenant ? C'est le moment d'utiliser votre identité SQRL en vous connectant et en créant des comptes sur les sites suivants :

- Le site de démonstration (en anglais) de SQRL de GRC (https://sqrl.grc.com/demo).
- Comment créer un nouveau compte sur ces forums avec SQRL (en anglais) (https://sqrl.grc.com/threads/how-to-register-a-new-account-on-these-forums-with-sqrl.267/).
- Le premier site de développement de SQRL détaillant des fonctions supplémentaire (en anglais) (https://www.grc.com/sqrl/demo.htm).

- Le site de GRC détaillant les fonctions de « gestion des accès partagés » (Managed Shared Access) (en anglais) (https://sqrl.grc.com/msa)

Il ne vous restera plus qu'à vous balader dans les forums pour en apprendre encore un peu plus sur SQRL !

Tout le monde ici est persuadé que SQRL représente l'avenir. Nous espérons que ce sera aussi votre avis ! Rejoignez-nous.

Questions/Réponses pour les utilisateurs

Une page destinée aux personnes utilisant déjà SQRL et qui ont des questions sur son utilisation.

Dans SQRL, quelle est la différence entre la fonction « Déverrouillage rapide » (QuickPass) et le Mot de passe (Password) ?

Les identités SQRL sont toujours protégées par un système de chiffrement (« cryptage ») de très haut niveau. À chaque fois qu'elle est utilisée, il est nécessaire que votre identité soit brièvement décryptée, juste pour un instant. C'est à ça que sert le mot de passe protégeant votre identité. Mais, une fois que votre identité a été décryptée, le système la chiffre de nouveau de manière temporaire en n'utilisant cette fois que les quelques premiers caractères du mot de passe. C'est vous qui décidez du nombre de caractères. Vous pouvez choisir de n'utiliser qu'un seul caractère, mais il est tout de même plus sûr d'en utiliser plusieurs. Ensuite, puisque que SQRL connaît le nombre de caractères de cette « version courte » du mot de passe, il vous suffit de taper ces quelques caractères pour que votre identité soit de nouveau déverrouillée les fois suivantes que vous utilisez SQRL pour vous authentifier. Autrement dit, la fonction de Déverrouillage rapide (QuickPass) a été créée pour faciliter l'utilisation répétée de SQRL sans subir la frustration d'avoir à rentrer votre long mot passe à chaque fois. Il n'y a en effet aucune raison de vous demander de retaper votre mot de passe complet toutes les quelques minutes. En revanche, ce mot de passe temporaire raccourci est désactivé automatiquement dès que l'économiseur d'écran se met en route, dès que vous verrouillez votre session ou votre ordinateur, ou dès que vous éteignez ce dernier.

À quoi sert le Code de secours (Rescue Code) de SQRL ?

Comme l'explique la réponse précédente, votre identité SQRL est chiffrée à l'aide de votre mot de passe. Mais votre identité est également chiffrée de manière encore plus forte avec votre Code de secours SQRL. Le mot de passe est utilisé pour votre utilisation quotidienne de SQRL. Personne ne s'attend à ce que vous reteniez par cœur votre Code de secours, mais il est capital que vous ne le perdiez pas ! Votre Code de secours a en effet plusieurs « super-pouvoirs » :

Il vous est sûrement déjà arrivé d'oublier le mot de passe d'accès à un site Web (comme à tout le monde n'est-ce pas ?). Vous avez alors dû demander au site Web de vous envoyer un courriel de récupération de mot de passe. Mais SQRL est super sécurisé car justement personne ne connaît votre mot de passe SQRL. Autrement dit si, par exemple, vous décidiez de le changer et qu'ensuite vous ne vous en souveniez plus, personne ne peut vous aider. Seul le Code de secours peut vous aider à sortir de cette situation et de quelques autres…

Si vous avez le moindre doute sur le fait que votre identité SQRL ait pu être compromise — par un malware, un pirate ou une quelconque agence gouvernementale — votre Code de secours vous permet en toutes circonstances de « réencrypter » votre identité à l'aide d'un nouveau mot de passe principal. Comme votre Code de secours est stocké « hors ligne », imprimé sur une feuille de papier quelque part, il est impossible pour quiconque de le récupérer depuis l'un de vos appareils, même si un pirate avait réussi à vous voler votre fichier d'identité SQRL. Cela signifie que vous êtes absolument la seule personne à pouvoir « réencrypter » votre identité SQRL. Une fois que vous avez « réencrypté » votre identité, tous les sites Web sur lesquels vous retournez vous reconnaîtront d'abord à l'aide de votre identité précédente (la longue suite de caractères qui vous représente), qu'ils remplaceront immédiatement par la nouvelle identité liée à votre nouveau mot de passe principal. Cela signifie que toute personne qui aurait malgré tout réussi à vous voler votre identité SQRL précédente ne pourrait en aucun cas l'utiliser pour se connecter à un site que vous auriez informé de votre nouvelle identité, ce que vous faites donc simplement en vous y connectant à l'aide de votre nouvelle identité « réencryptée ».

Si jamais vous n'avez pas la possibilité de « réencrypter » votre identité immédiatement —par exemple parce que vous n'avez pas votre Code de secours sous la main– et de vous connecter aux sites Web qui l'utilisent pour les informer de votre nouvelle identité, vous pouvez utiliser votre identité SQRL compromise pour désactiver la fonction d'authentification via SQRL sur chacun des sites qui l'utilisent. Cela en interdira donc l'accès également à votre voleur d'identité car une fois que l'authentification SQRL est désactivée, plus personne ne peut utiliser cette identité (pas même vous) pour la réactiver. La réactivation requiert en effet l'utilisation du Code de secours. Cela signifie que vous pouvez donc choisir, en cas de besoin, de redonner le droit à votre identité SQRL compromise de vous réauthentifier sur un site Web. Mais il vaut mieux « réencrypter » votre identité pour que celle qui a été compromise ne soit plus jamais utilisée. Et SQRL vous permet de le faire très facilement.

Le niveau de sécurité de votre Code de secours est si élevé qu'il n'est affiché que très brièvement sur l'écran de l'appareil à partir duquel vous créez votre identité SQRL. Vous DEVEZ ensuite l'écrire ou l'imprimer sur une feuille de papier, que vous stockerez dans un endroit sûr. Si tout se passe correctement, vous n'en aurez jamais besoin. Mais vous serez très content d'en disposer le jour où vous en aurez besoin !

Que dois-je sauvegarder pour assurer la sécurité du système ?

En résumé : votre identité SQRL et votre Code de secours. C'est tout.

Vous pouvez sauvegarder (exporter) votre identité à tout moment en l'imprimant ou en l'enregistrant dans un fichier. Votre identité est chiffrée, vous pouvez donc la stocker en toute sécurité sur une clé USB. Cela dit, rien ne vaut la sécurité hors-connexion d'une copie papier. C'est pourquoi nous vous recommandons d'exporter votre identité en l'imprimant. Comme il est très probable que votre identité SQRL soit installée sur plusieurs appareils —votre(vos)

ordinateur(s), votre(vos) appareil(s) mobile(s)— le risque que vous perdiez votre identité est très faible puisque chaque appareil sert en quelque sorte de sauvegarde pour les autres. Cela dit, comme il est indiqué dans la réponse précédente, votre Code de secours est différent et spécial. Ce Code de secours est si sécurisé qu'il n'est visible que pendant un moment très bref lors de la création de votre identité SQRL. Il n'est jamais stocké sur aucun de vos appareils et ne devrait d'ailleurs jamais l'être. Vous devez absolument l'écrire ou l'imprimer pour le conserver en toute sécurité hors-connexion.

Si vous suivez ces quelques règles, vous pourrez utiliser votre identité SQRL, sans aucune inquiétude, pour toujours.

Lorsque j'exporte mon identité SQRL, dois-je le faire avec ou sans mon mot de passe ?

Une identité SQRL exportée peut toujours, sans exception, être décryptée à l'aide du Code de secours. Mais, pour une utilisation simplifiée, l'exportation d'une identité peut aussi inclure son mot de passe. Cela permet d'importer et d'utiliser cette identité sur d'autres appareils sans avoir besoin de recourir au Code de secours. Cela dit, puisqu'une identité peut-être décryptée avec son mot de passe, il est beaucoup moins sécurisé d'archiver des copies de son identité SQRL accompagnée du mot de passe qui lui correspond. Il y a donc deux cas de figure. Si vous exportez votre identité pour l'utiliser immédiatement sur un autre appareil, il est bien plus pratique de l'exporter avec son mot de passe. En revanche, si vous l'exportez pour l'archiver et la protéger, ne pas inclure son mot de passe dans l'exportation rendra bien plus difficile la vie d'un éventuel pirate qui tenterait de casser le chiffrement de l'identité.

Quand peut-il être nécessaire de créer une autre identité SQRL ?

Quasiment jamais. Internet nous a donné l'habitude de créer de multiples identifiants, habitude difficile à combattre. Mais comme les sites Web ne connaissent leurs visiteurs SQRL que sous la forme d'une longue suite de caractères de la forme « E6Qs2gX7W-Pwi9Y3Kam-kuYjLSWXCt-yBcymWl-HAuo », unique pour chaque site, tous les utilisateurs SQRL sont anonymes. Il n'y aucun moyen de devenir « plus » anonyme que ça. Si votre raison pour créer une nouvelle identité repose sur un besoin de pouvoir utiliser un compte différent sur un même site Web, SQRL inclut déjà pour ça la fonction d'« Alt-ID » (voir question suivante).

Les Identités Alternatives (Alt-IDs), c'est quoi ?

Il peut arriver que vous ayez besoin de vous connecter à un site Web comme un utilisateur que le site Web ne connaît pas encore —un alter ego. Du temps du vieux système d'identifiant et mot de passe, il fallait créer un nouveau compte en inventant un nouvel identifiant, afin de pouvoir passer pour quelqu'un d'autre. C'est ce que permet de faire la fonction d'Identité Alternative (Alt-ID) de SQRL. À tout moment, vous pouvez utiliser une identité alternative pour vous connecter à un site Web en tant qu'utilisateur SQRL différent. Les identités alternatives ne sont que du texte que vous tapez au clavier, n'importe quel texte. Vous pouvez créer autant d'Alt-ID que vous voulez. Et si vous utilisez le même texte lorsque vous revenez sur un site auquel vous avez déjà rendu visite, vous serez reconnu comme étant la même « autre » personne.

Que signifie l'option « Request only SQRL sign in » (Demander de n'accepter que l'authentification par SQRL) ?

Le système d'authentification de SQRL est non seulement bien plus pratique que les traditionnels identifiants et mots de passe, il est aussi bien plus sécurisé. Mais si les deux méthodes d'authentification restent disponibles, les pirates tentant de s'introduire dans votre compte ont donc toujours la possibilité de contourner SQRL en utilisant l'identifiant et le mot de passe d'un utilisateur pour se connecter. La fonction « Request only SQRL sign in » est la solution à ce problème. Une fois que vous vous sentez à l'aise avec l'utilisation de SQRL, et que vous avez imprimé et mis bien à l'abri votre identité SQRL et votre Code de secours, vous pouvez faire en sorte de demander à ce que tous les sites que vous visitez n'acceptent que SQRL comme méthode d'authentification. Lorsque vous vous reconnecterez avec cette option activée, le site Web devrait reconnaître cette demande et s'en souvenir pour les fois suivantes. Il s'agit uniquement d'une demande car SQRL ne peut pas obliger les sites Web à désactiver toutes les autres méthodes d'authentification. Mais les utilisateurs de SQRL peuvent facilement vérifier qu'un site accède ou non à la demande simplement en essayant de se connecter avec leurs identifiant et mot de passe précédents. Si cela fonctionne toujours, les utilisateurs SQRL peuvent alors s'adresser aux responsables du site pour leur demander d'honorer la demande d'authentification uniquement par SQRL.

Que signifie l'option « Request no account recovery » (Demander la désactivation de la récupération de compte) ?

Il s'agit d'un complément de la problématique précédente. Si une fonction de « récupération de compte » de quelque forme que ce soit est proposée par un site Web, alors un pirate qui aurait réussi à prendre possession de votre compte de courriel pourrait sans problème utiliser l'option « J'ai oublié mon mot de passe » pour obtenir un lien permettant de réinitialiser le mot de passe. Cela arrive tous les jours. Autrement dit, dès que vous vous sentez à l'aise avec l'utilisation de SQRL, et que vous avez imprimé et mis bien à l'abri votre identité SQRL et votre Code de secours, vous pouvez activer cette option pour demander aux sites Web de désactiver leur fonction de récupération de compte, qu'elle soit automatique ou via un service d'assistance. Il n'y aucune raison que vous n'ayez pas le droit d'en prendre la responsabilité si vous le voulez.

Et si jamais je PERDS mon Code de secours ?

Il est capital que vous ne perdiez pas votre Code de secours. Il ne peut jamais être récupéré ou recréé. Il est probable que vous puissiez utiliser SQRL pendant toute votre vie sans jamais avoir besoin de votre Code de secours ne serait-ce qu'une seule fois, si vous n'oubliez jamais le mot de passe de votre identité SQRL et si vous n'avez jamais besoin de la « réencrypter ». Mais si vous voulez vraiment vous engager sérieusement dans l'utilisation de SQRL, il est indispensable de conserver votre Code de secours.

Cela dit, admettons que vous ayez créé une identité SQRL dans les tout débuts, au moment de sa création, sans la prendre suffisamment au sérieux, et que vous avez perdu ou égaré votre Code de secours. Soulignons tout d'abord que si vous ne vous souvenez plus de l'endroit où vous avez rangé votre Code de secours imprimé, il vaut peut-être mieux ne pas continuer à

utiliser votre identité SQRL au cas où quelqu'un d'autre aurait trouvé votre Code de secours. Du coup…

1. Avant toute chose, créez une nouvelle identité SQRL de remplacement que vous prendrez cette fois au sérieux. Imprimez-la, ainsi que votre Code de secours et stockez-les séparément dans un endroit sûr dont vous vous souviendrez.

Si les sites SQRL que vous visitez sont compatibles avec la fonction MSA (Managed Shared Access - Gestion des accès partagés), vous pourrez gérer vous-même le remplacement de votre ancienne identité SQRL devenue inutile :

1. Connectez-vous avec l'ancienne identité SQRL que vous allez abandonner.
2. Rendez-vous sur la page MSA du site et créez une invitation disposant des droits d'« administrateur ».
3. Déconnectez-vous du site sur lequel vous aviez utilisé l'ancienne identité.
4. Ré-authentifiez-vous à l'aide de la nouvelle identité et utilisez l'invitation pour retrouver l'accès à votre compte.
5. Servez-vous de vos droits d'administration pour détruire l'identité SQRL que vous abandonnez. Vous obtiendrez alors le droit de propriété sur le compte que vous aviez ouvert sur ce site.

Vous devrez suivre cette procédure sur chacun des sites compatibles MSA sur lesquels vous utilisez SQRL. Ce n'est pas automatique, mais ça fonctionne… c'est garanti. Pour les sites qui ne proposent pas cette Gestion des accès partagés, vous aurez besoin d'une autre méthode.

Vous devrez :

1. Vous connecter aux sites qui utilisent l'identité SQRL que vous souhaitez abandonner en ayant au préalable pris soin de désactiver les options « Request only SQRL sign in » (Demander de n'accepter que l'authentification par SQRL) et « Request no account recovery » (Demander la désactivation de la récupération de compte) afin de réduire votre niveau de sécurité et que toutes les possibilités de récupération de l'accès au compte soient disponibles.
2. Contacter l'administrateur du site et utiliser les moyens qu'il met à votre disposition pour remplacer une identité SQRL perdue ou à laquelle vous ne faites plus confiance. Cette démarche est normalement contraire à la politique d'utilisation de SQRL puisque le système est bâti sur l'utilisation du Code de secours. Mais, au moins pendant la période de lancement de SQRL, nous estimons que si un utilisateur SQRL parvient à convaincre un site Web qu'il est bien le propriétaire du compte dont il veut transférer l'accès à une autre identité SQRL —par exemple en montrant qu'il est toujours en possession de ses anciens identifiant et mot de passe et du courriel de récupération, alors il semble raisonnable qu'un site puisse être enclin à apporter de l'aide à son utilisateur.

Comment puis-je me familiariser un peu plus avec SQRL ?

La meilleure façon de se sentir plus à l'aise avec SQRL c'est encore de l'utiliser. Vous pouvez vous connecter à ce forum en utilisant SQRL et GRC dispose d'une page de démonstration accessible depuis l'adresse suivante (en anglais) : https://sqrl.grc.com/demo. Et si vous voulez essayer les fonctions plus avancées de Gestion des accès partagés (Managed Shared Access, MSA), vous pouvez vous rendre sur https://sqrl.grc.com/msa (page en anglais). Et… ces forums regorgent d'utilisateurs de SQRL, dont beaucoup ont travaillé et contribué à son développement pendant de nombreuses années. N'hésitez donc pas à y poser des questions. C'est là que vous trouverez des réponses.

Ces pages de Questions/Réponses devraient permettre à tout nouvel utilisateur de SQRL d'en comprendre les fonctions les plus importantes. Pour détailler des scénarios d'utilisation plus complexes, reportez-vous à notre page « Mais, et si… » (disponible en anglais uniquement pour le moment : https://sqrl.grc.com/pages/whatif/).

Oui, mais… et si ?

Une liste aussi exhaustive que possible de toutes les situations du type « Et si j'utilise SQRL et que… » et les réponses qui vont avec.

Et si j'utilise SQRL. Cela signifie que l'on ne peut plus me suivre à la trace ?

Non. Les mécanismes traditionnels de suivi sur Internet restent fonctionnels. SQRL ne peut pas empêcher le suivi, mais au moins, il ne fournit aucune information supplémentaire susceptible d'être utilisée pour vous suivre à la trace. Combien de sites Web se basent sur votre adresse de courriel pour vous identifier ? Les annonceurs et autres publicitaires sont en position de récupérer votre adresse de courriel pour suivre ensuite vos pérégrinations de site en site. Avec SQRL, chaque site Web reçoit de votre part un « charabia » créé au hasard et différent pour chaque site Web que vous visitez. Autrement dit, SQRL ne donne aucune information qui permette de vous suivre d'un site à l'autre.

Et si ma banque a absolument besoin de s'assurer que c'est bien moi qui approuve une opération importante ?

Bonne question, parce que justement SQRL le permet également. Même si le système n'est pas à proprement parler conçu pour vous identifier, il est en revanche conçu pour certifier de manière absolument sûre votre intention et/ou l'obtention d'une permission pour réaliser en ligne quelque chose d'important. Le système SQRL inclut une fonction appelée « Ask » (Demander) qui permet à un site Web de vous « poser une question » lorsqu'il a besoin d'obtenir de votre part une approbation claire et explicite.

Par exemple, si vous demandez à votre banque d'effectuer un virement de 200 000 € vers un compte avec lequel vous n'avez encore eu aucune interaction, votre banque, détectant que vous êtes un utilisateur de SQRL, peut afficher un message du type « Cliquez pour confirmer avec SQRL », ou un code QR dans le même but. À ce moment-là, votre appli SQRL affiche une boîte de dialogue supplémentaire contenant la question que vous pose la banque, comme par exemple: « Merci de confirmer le transfert de 200 000 € vers le compte n° 123-234-345-456 ». Si besoin, la banque peut également ajouter un ou deux boutons pour compléter votre réponse. Et cette réponse étant signée électroniquement par votre application SQRL, elle ne peut provenir que de vous. Autrement dit, cette méthode est BIEN PLUS sécurisée que de simplement cliquer sur un bouton « Oui, je suis sûr », sur lequel un virus contenu dans la page Web pourrait cliquer à. votre place sans même que vous ne vous en rendiez compte.

Et si SQRL n'est pas disponible sur l'appareil ou le système d'exploitation que j'utilise ?

L'utilisation d'une application est indispensable. À l'inverse des systèmes reposant sur l'utilisation d'un identifiant et d'un mot de passe, SQRL a absolument besoin d'une application pour vous connecter un service en ligne. Il n'y a pas d'autre moyen. De nouvelles applications SQRL sont toujours en développement. Consultez régulièrement la page « Bien démarrer » sur ce forum (ou dans ce document) pour découvrir les nouvelles versions d'application disponibles.

SQRL est également disponible sous forme d'une extension pour les navigateurs Internet Google Chrome, Microsoft Edge ou Firefox. S'il n'existe encore aucune application SQRL pour votre système, vous pouvez tout de même utiliser SQRL grâce à ces extensions.

Il est très probable qu'à terme, les fonctions de SQRL seront intégrées aux gestionnaires de mots de passe, aux navigateurs ou même aux systèmes d'exploitation. SQRL est libre et gratuit et n'importe qui peut donc décider de l'intégrer à l'outil ou système qu'il/elle développe.

Et si j'oublie mon mot de passe SQRL ?

Votre Code de secours SQRL peut à tout moment être utilisé pour modifier le mot de passe lié à votre identité SQRL. Même si vous n'avez pas besoin de votre Code de secours pour votre utilisation quotidienne de SQRL, et que vous n'aurez peut-être jamais à vous en servir, vous devez absolument le conserver en lieu sûr, en l'imprimant ou en l'écrivant quelque part (votre journal, un endroit chez vous ou n'importe quel autre endroit sûr…). Vous serez content de l'avoir le jour où vous en aurez besoin.

Et si j'utilise plusieurs ordinateurs et/ou smartphones ?

Une seule identité SQRL est nécessaire pour chaque utilisateur de SQRL, identité qui peut être facilement partagée entre tous ses appareils (ordinateurs, tablettes, smartphones). Toutes les applications SQRL sont capables d'afficher l'identité SQRL qu'elles hébergent sous la forme d'un QR code qui peut ainsi être scanné par n'importe quel autre appareil ou imprimé sur une feuille de papier incluant à la fois le QR code et une chaîne de caractères représentant l'identité.

Autrement dit, votre identité SQRL créée sur un premier appareil peut ensuite être « exportée » depuis ce premier appareil vers tous vos autres appareils. La meilleure façon de faire consiste à

utiliser la fonction d'exportation avec le mot de passe, afin que le même mot de passe puisse être utilisé sur le ou les autres appareils lorsque vous avez besoin de vous authentifier.

C'est à vous de faire en sorte que tous vos appareils utilisent le même mot de passe pour votre identité SQRL. SQRL ne le fait pas pour vous, et ne peut pas le faire pour vous. Si vous changez le mot de passe de votre identité SQRL sur un de vos appareils, ce que vous pouvez choisir de faire quand bon vous semble, le mot de passe ne sera PAS modifié automatiquement sur vos autres appareils. Aussi, afin d'éviter toute confusion, il vaut mieux changer le mot de passe sur tous ses appareils en même temps pour toujours n'en avoir qu'un à garder en mémoire.

Le principe est le même lorsque vous pensez avoir besoin de « réencrypter » votre identité. Ce qui peut arriver si vous pensez que votre identité SQRL a pu être compromise, volée ou tombée entre dans de mauvaises mains. Si vous réencryptez votre identité SQRL sur un de vos appareils, elle ne sera PAS automatiquement réencryptée sur les autres. Ce n'est pas vraiment un problème pour l'utilisateur car il n'est normalement jamais nécessaire de réencrypter une identité SQRL. Mais cette fonction est tout de même disponible pour les rares cas où vous en ressentez le besoin.

Cela dit, si jamais vous effectuez l'opération de « réencryptage » de votre identité SQRL sur l'un de vos appareils, vous ne pouvez pas, et ne devez pas, lancez cette même opération sur vos autres appareils puisque cela créerait une clé différente sur chacun d'eux. La bonne manière de faire consiste alors à exporter l'identité qui vient juste d'être réencryptée pour l'importer sur tous les autres appareils sur lesquels vous souhaitez utiliser votre identité SQRL. Exactement comme lorsque vous vous avez créé votre identité pour la première fois et que vous avez utilisé le QR code pour en équiper vos autres appareils. Bref, il vous suffit de d'utiliser les fonctions « d'import/export » de votre identité SQRL, comme la première fois.

Afin de pouvoir réencrypter votre identité SQRL, vous devez disposer du Code de secours de votre identité SQRL. À la fin de la procédure de « réencryptage », un nouveau Code de secours vous sera donné, lié à la nouvelle clé de chiffrage de votre identité SQRL. Ne détruisez pas pour autant la feuille de papier sur laquelle vous aviez conservé le Code de secours précédent. Imprimez le nouveau Code de secours et stockez-le au même endroit, au cas où vous en auriez besoin plus tard.

Et si je partage un appareil qui ne connaît pas la notion de comptes utilisateurs différents comme un iPad ou un iPhone ?

Bien qu'un utilisateur de SQRL n'ait besoin que d'une seule identité SQRL, chaque utilisateur SQRL a besoin de sa PROPRE identité. Lorsque l'on utilise un système multi-utilisateur comme Windows, macOS ou Linux, chaque compte utilisateur sur la machine peut héberger l'identité SQRL de cet utilisateur. Mais, effectivement, les appareils personnels tels que ceux d'Apple, ne disposent d'aucune fonction multi-utilisateur de ce type.

Les applications SQRL pour ces appareils permettent de créer ou d'importer plusieurs identités SQRL. Il suffit ensuite de sélectionner celle que vous souhaitez utiliser lorsque vous avez besoin de vous authentifier sur un site Web. Comme il ne s'agit pas d'un besoin courant, cette fonction de sélection d'utilisateur se situe le plus souvent dans les paramètres de l'application SQRL, afin de ne pas perturber la grande majorité des utilisateurs. Mais cette fonction est donc disponible si vous en avez besoin.

Et si j'ai besoin d'importer mon identité SQRL sur un PC qui n'a pas de webcam ?

Et c'est le cas de la majorité des PC de bureau n'est-ce pas ? C'est prévu. En plus de fournir un QR code à scanner, les applications SQRL peuvent produire des versions « texte » imprimées d'une identité, et même les exporter dans un fichier. Commencez donc par vérifier si l'un de vos appareils vous propose l'option d'exporter votre identité SQRL vers un fichier. Si c'est le cas, transférez alors ce fichier vers votre PC sans webcam et importez votre identité de cette manière dans l'application SQRL de ce PC.

Si le transfert de ce fichier n'est pas possible, vous pouvez imprimer votre identité SQRL depuis n'importe quel appareil, pour ensuite tout simplement taper au clavier l'identité SQRL représentée par une suite unique de caractères. Bien sûr, ce n'est pas très rapide, mais le système vous aide en vérifiant votre saisie ligne à ligne. Et vous n'aurez à réaliser cette saisie qu'une seule fois. Pour en réduire la taille, cette suite de caractères n'inclut pas les informations liées à votre mot de passe. Vous aurez donc besoin du Code de secours pour valider l'importation « à la main » de votre identité SQRL dans une autre application SQRL.

Et si quelqu'un parvient à pirater mon téléphone et récupère mon identité ?

Toutes les identités SQRL sont fortement chiffrées à l'aide d'un procédé délibérément lent, demandant au moins quelques secondes pour chaque essai. Ce qui signifie que cela rend quasi impossible à un pirate qui aurait récupéré le fichier de votre identité de deviner votre mot de passe en essayant toute les possibilités les unes après les autres. Autrement dit, plus votre mot de passe est long et complexe, plus il sera difficile à n'importe qui de le « craquer ». Et personne, pas même vous, ne peut utiliser votre identité sans son mot de passe associé.

Et si quelqu'un parvient à s'emparer à la fois de mon identité ET de mon mot de passe ?

Si un pirate malveillant parvenait à récupérer votre identité ET votre mot de passe, alors il pourrait effectivement se faire passer pour vous sur n'importe quel site Web qui vous reconnaît à l'aide de votre identité SQRL. Heureusement, SQRL dispose d'une fonction vous permettant de bloquer ce pirate et de récupérer votre identité, même dans cette situation catastrophique. Aucun pirate ne peut mettre la main sur votre Code de secours puisque ce dernier est stocké de manière sécurisée, hors connexion, et jamais sur aucun de vos appareils. Ce Code de secours vous permet de réencrypter votre identité pour la récupérer et en retirer l'accès et l'usage des mains d'un pirate ou d'une quelconque autorité gouvernementale qui s'en serait emparé sans votre permission.

Une fois votre identité réencryptée, votre application SQRL contiendra les deux versions de votre identité. La version précédente est conservée afin que les sites Web sur lesquels vous vous rendez puissent continuer à vous reconnaître. Mais ils verront également que vous disposez d'une nouvelle version de cette même identité. Ils commenceront automatiquement à utiliser cette nouvelle version et oublieront totalement l'ancienne. Dès lors, quiconque tenterait de se connecter sur ce site Web avec l'ancienne version de votre identité serait tout simplement ignoré.

Cela signifie qu'après avoir réencrypté votre identité SQRL, il vous faut vous connecter à tous les sites Web avec lesquels vous utilisez SQRL (notamment les plus importants comme votre banque, vos réseaux sociaux principaux, les sites de commerce que vous utilisez, etc.) pour automatiquement remplacer l'ancienne version de votre identité par la nouvelle. Le tour est joué, même si quelqu'un avait acquis la possibilité de se faire passer pour vous avec l'ancienne version de votre identité, celle-ci devient inutilisable sur tous les sites que vous avez informés de la nouvelle version de votre identité.

Et si je me trouve dans la situation précédente, mais que je n'ai pas accès à mon Code de secours me permettant de réencrypter mon identité ?

C'est prévu également. Si vous pensez que votre identité SQRL est compromise, mais que vous n'avez pas la possibilité de la réencrypter puis de visiter vos sites Web habituels dans la foulée, vous avez au moins la possibilité de désactiver l'usage de votre identité sur tous les sites qui l'utilisent, sans avoir besoin de votre Code de secours. Une des fonctions de connexion de SQRL vous permet justement de désactiver l'usage de SQRL sur le site auquel vous êtes en train de vous connecter. Cette option est utilisable sans le Code de secours, mais l'inverse n'est pas vrai : le Code de secours sera ensuite indispensable pour réactiver l'authentification au site à l'aide de SQRL. Donc, si vous avez un doute sur l'utilisation non voulue de votre identité et que vous n'avez pas accès à votre Code de secours, vous pouvez au moins bloquer l'accès à quiconque, vous y compris, aux sites les plus importants. Une fois que vous avez récupéré l'accès à votre Code de secours, vous pouvez choisir de réactiver l'accès à ces sites via SQRL ou de réencrypter votre identité pour en créer une nouvelle version qui remplacera celle pour laquelle vous avez un doute, comme dans la question précédente.

Et si je perds ou je me fais voler l'ordinateur, la tablette ou le téléphone sur lequel mon identité SQRL est stockée?

Le système de chiffrement très robuste des identités SQRL les protège des tentatives de découverte au hasard du mot de passe qui les protège. Il est impossible pour quiconque, pas même vous, de raccourcir les 5 secondes que vous devez attendre pendant que l'application vérifie que le mot de passe que vous venez d'entrer est bien le bon. Ce qui signifie également que quiconque serait tenté d'essayer de trouver votre mot de passe en les testant tous serait vite frustré.

Puisque vous aurez imprimé et conservé votre Code de secours au moment de la création de votre identité SQRL, vous pourrez importer cette identité sur n'importe quel appareil qui remplacerait celui auquel vous n'avez plus accès, vous permettant ainsi de continuer à utiliser la même identité sans rien perdre de vos accès habituels. Si votre identité est installée sur l'un de vos appareils, vous pouvez la transférer d'un appareil à l'autre, comme vous l'avez probablement déjà fait pour pouvoir l'utiliser sur plusieurs appareils à la fois.

Et si vous avez le moindre doute sur le fait qu'une personne ayant volé votre appareil puisse malgré toutes les précautions prises deviner votre mot de passe et l'utiliser, il vous suffit d'utiliser votre Code de secours pour « réencrypter » votre identité SQRL puis de rendre visite à tous les

sites qui l'utilisent pour que la nouvelle version de votre identité remplace l'ancienne, rendant inopérante celle stockée sur l'appareil volé.

Et si j'ai perdu mon Code de secours et que j'en ai maintenant besoin ?

Malheureusement, le Code de secours de votre identité ne peut pas être récupéré ni recréé. Il faut absolument le considérer pour ce qu'il est : un secret irremplaçable qui n'est révélé qu'une seule et unique fois au moment de la création de l'identité. La seule solution consiste à créer une nouvelle identité SQRL, dont vous protégerez le Code de secours efficacement, pour ensuite demander aux sites auxquels vous vous connectez à l'aide de votre identité SQRL de bien vouloir vous laisser utiliser cette nouvelle identité pour vous connecter, à la place de l'ancienne.

Autrement dit, il est vraiment indispensable d'imprimer, de sauvegarder, de protéger et de ne pas perdre votre Code de secours. En faisant ça, vous l'aurez donc à disposition le jour où vous en avez besoin, ce qui vous permettra d'utiliser la même identité SQRL pour votre vie entière.

Et si je veux vérifier mon Code de secours ?

Vous avez besoin de votre Code de secours si vous souhaitez modifier le mot de passe oublié de votre identité SQRL. Autrement dit, la façon la plus simple de vérifier votre Code de secours est de l'utiliser pour essayer de changer le mot de passe. Une fois que vous avez vérifié que le Code de secours dont vous disposez est bien le bon, vous pouvez annuler la procédure de changement de mot de passe pour conserver celui que vous connaissez.

Et si j'ai besoin de partager un compte avec quelqu'un d'autre ?

Avec le système d'identifiant et mot de passe, partager l'accès à un site Web est aussi simple que de partager les identifiant et mot de passe de ce compte. Mais cela ne fonctionne que si vous utilisez un couple identifiant/mot de passe unique « par site Web ». SQRL est un système « par personne ». Il n'y a donc aucun moyen de partager l'identité SQRL d'une personne pour une partie seulement des sites Web sur lesquels vous vous authentifiez à l'aide de votre identité SQRL. Idéalement, la fonction de Gestion des Accès Partagés (*Managed Shared Access* - MSA) peut être utilisé par les sites Web pour permettre à plusieurs utilisateurs SQRL de se connecter au même site. On espère donc que tous les sites Web pour lesquels le partage de compte a un sens adopteront le système MSA de SQRL.

Si plus d'un utilisateur a besoin de s'authentifier auprès de sites qui ne sont pas compatibles avec le MSA, la seule solution consiste alors, en tout cas jusqu'à ce que les sites concernés adoptent cette fonction importante, à créer une autre identité SQRL à partager pour se connecter aux sites qui ne sont pas compatibles avec le principe des identités multiples. Par exemple, les deux parents d'un foyer peuvent créer une identité SQRL « parentale » qu'ils utilisent pour se connecter à leur banque ou aux compagnies de gaz et d'électricité par exemple. Petit à petit cette identité partagée pourra être utilisée avec tous les comptes en ligne de la famille qu'ils voudront. Au fur et à mesure que les sites adopteront le système SQRL complet, c'est-à-dire compatible avec le MSA, les identités parentales individuelles pourront être ajoutées à chacun des comptes, et l'identité parentales partagée pourra être mise au rebut.

Et si je veux changer l'identité SQRL d'un site Web (avec Gestion des accès partagés - MSA) ?

Les site Web qui sont entièrement compatibles avec SQRL, le seront également avec la fonction MSA (Managed Shared Access ou Gestion des accès partagés). Cette fonction permet à plusieurs identités SQRL de servir d'authentifiant pour un seul compte sur un site Web. Donc, lorsqu'un site auprès duquel vous souhaitez changer d'identité SQRL est pleinement compatible, il vous suffit d'ajouter la nouvelle identité SQRL au compte avant d'en supprimer l'ancienne.

Et si je veux changer l'identité SQRL d'un site Web (sans Gestion des accès partagés - MSA) ?

Pour les sites Web qui ne sont pas pleinement compatibles avec SQRL et qui notamment n'offrent pas la fonction MSA, l'application SQRL inclut une fonction vous permettant d'effacer ou de remplacer une identité auprès d'un serveur. On peut par exemple supprimer une identité SQRL d'un site en utilisant son Code de secours. Mais cette procédure ne déconnecte pas le propriétaire de l'identité SQRL du compte concerné. Donc, dès que l'ancienne identité a été supprimée du site Web, celle de remplacement peut être ajoutée immédiatement au compte et le tour est joué : l'ancienne identité est oubliée sur ce site Web, remplacée par la nouvelle.

Et si j'ai créé plusieurs identités SQRL et que je veux les fusionner?

Si, pour quelque raison que ce soit vous utilisez plusieurs identités SQRL et que vous souhaitez les fusionner pour n'en conserver qu'une, il vous suffit de faire l'échange d'identité SQRL auprès de chaque site Web concerné, en suivant les instructions des deux questions précédentes, jusqu'à ne plus avoir qu'une seule identité en service.

Et si je veux utiliser une autre identité sur un site qui me connaît déjà ?

SQRL inclut une fonction connut sous le nom d'identités alternatives ou Alt-ID qui permet justement de faire exactement ça : faire en sorte qu'un site Web vous considère comme quelqu'un d'autre alors même que vous utilisez la même identité SQRL. Cela évite d'avoir à créer une nouvelle identité SQRL pour ce seul besoin. Vous créez une Alt-ID depuis votre identité principale et le texte que vous choisissez devient votre « nom alternatif ».Et si vous souhaitez réapparaître comme votre même« alter-SQRL » auprès d'un site que vous visitez de nouveau, il vous suffit d'utiliser exactement le même texte. Soulignons ce détail : le texte que vous utilisez pour votre Alt-ID doit être absolument identique, sinon le site considérera qu'il s'agit de nouveau d'un nouveau visiteur. Mieux vaut donc se cantonner à un nom simple comme par exemple « Deux » ou « Anonyme ». Dans ce cas précis, un nom court n'a aucune incidence sur le niveau de sécurité puisqu'il ne s'agit que d'appliquer une étiquette temporaire à votre identité SQRL dont le niveau de sécurité n'est pas modifié.

Et si j'utilise une application SQRL malveillante?

Pour le dire gentiment, ce serait ennuyeux ! Cela serait similaire à l'utilisation d'un gestionnaire de mots de passe malveillant qui enverrait tous vos identifiants de connexion à quelqu'un d'autre. La

seule façon de vous prémunir de ce problème consiste à choisir TRÈS attentivement les applications SQRL que vous utilisez.

Avec SQRL, on peut considérer que le danger est même plus grand encore : si une application SQRL malveillante parvenait à récupérer votre identité et son mot de passe, alors un malfaiteur pourrait se faire passer pour vous auprès, non seulement, de tous les sites sur lesquels vous avez déjà un compte, mais aussi des sites dont vous pourriez avoir l'usage plus tard.

Si jamais vous découvrez que l'application SQRL que vous utilisez est malveillante, la première chose à faire consiste à l'effacer et à en obtenir une autre digne de confiance. Il vous faudra ensuite suivre la procédure de « réencryption » de votre identité, puis rendre visite à tous les sites importants afin que ces derniers utilisent la nouvelle version de votre identité et oublient la version précédente compromise). Comme l'application SQRL malveillante ne serait pas en possession de votre Code de secours, celle-ci ne serait pas en mesure de vous effacer de ces sites ou de procéder elle-même à la « réencryption » de votre identité. Seul votre Code de secours a le pouvoir de le faire.

Cela dit, l'utilisation d'une application SQRL qui ne serait pas digne de confiance est ce que l'on peut imaginer de pire. Il est donc VRAIMENT préférable de ne pas prendre ce risque. SURTOUT, n'utilisez que les applications SQRL reconnues et recommandées sur ce site Web, et évitez TOUTES celles qui ne sont pas reconnues de manière générale comme étant acceptées et de confiance. Aucune fonction prétendument séduisante ne l'est suffisamment pour courir ce risque.

Et si quelqu'un s'identifie sur un site en scannant un QR Code par dessus mon épaule, sans que je m'en aperçoive?

Imaginons que votre écran affiche la page de connexion à un site Web et que quelqu'un derrière vous se serve de son propre smartphone pour scanner le QR code SQRL. Et si, cela peut arriver.

À vrai dire, on ne voit pas bien l'intérêt d'une telle action puisqu'elle entraînerait tout simplement la connexion de cette autre personne, via sa propre identité SQRL, dans le navigateur Internet que vous êtes en train d'utiliser. Autrement dit, cela n'a aucune incidence sur la sécurité de votre propre identité ou de votre compte sur le site Web concerné. Donc, oui, c'est possible. Mais cela ne peut vous nuire en aucun cas et n'a aucun sens pour la personne qui le ferait. Bref, il s'agit juste d'une utilisation absurde de la méthode d'authentification de SQRL.

Et si je tape mon Code de secours dans une application SQRL malveillante ?

Commençons par le plus important : ne le faites jamais. Sérieusement. Jamais.

Comme indiqué un peu plus haut, il est CAPITAL d'utiliser uniquement des applications SQRL de confiance. La page « Bien démarrer avec SQRL » de ce forum fournit une liste des applications que nous avons examinées, et dont les auteurs et leur travail sont connus et recommandés. Réfléchissez y à deux fois, S'IL VOUS PLAÎT, avant d'utiliser une application SQRL qui ne serait pas listée ici. Faites vos propres recherches. Il est évident que des applications SQRL malveillantes seront créées vu l'immense service qu'elles pourraient rendre à leurs auteurs. Répétons-le donc, S'IL VOUS PLAÎT, soyez extrêmement prudent. Si une application SQRL n'est

pas répertoriée ici, ne l'installez pas tout de suite et commencez par une enquête approfondie sur la réputation de son auteur et du site qui la publie (et pourquoi pas, posez donc une question sur ce forum demandant pourquoi cette application n'y est PAS proposée).

Cela dit, en cas d'utilisation d'une application malveillante, il n'y a aucun moyen de savoir ce qu'elle fait. On peut tout imaginer. Autrement dit, il est bien difficile dans ces conditions de donner de bons conseils pour s'en sortir. Première étape : cesser immédiatement d'utiliser des applications SQRL qui ne sont pas dignes de confiance.

Si votre identité SQRL est enregistrée dans une autre application SQRL, digne de confiance elle, utilisez cette dernière pour réencrypter votre identité et ainsi en récupérer l'usage exclusif. Si ce n'est pas le cas, installez sans tarder une application digne de confiance, importez-y votre identité grâce à votre sauvegarde papier par exemple, et ensuite procéder à la réencryption de votre identité. Rendez-vous ensuite sur tous les sites sur lesquels vous l'utilisez pour remplacer l'ancienne version compromise de votre identité par la nouvelle (voir plus haut). C'est ainsi que vous BLOQUEREZ à coup sûr l'utilisation de l'ancienne version de votre identité par l'application malveillante.

Tous les sites sur lesquels vous vous identifierez à l'aide de la nouvelle version réencryptée de votre identité, détruirons l'ancienne version et vous aurez donc « repris la main » sur votre identité SQRL un temps compromise.

Et si je perds la sortie papier de mon identité ?

Toutes les applications SQRL ont la possibilité d'exporter ou d'imprimer votre identité à tout moment. Utilisez donc l'une de celles que vous avez installées pour générer de nouveau la page de secours de l'identité et du mot de passe que vous êtes en train d'utiliser, afin d'en récupérer une sauvegarde sécurisée hors connexion. Autrement dit, même si vous avez perdu la première feuille imprimée au moment de la création de votre identité, il est très facile d'en imprimer une autre.

Attention, cette méthode ne s'applique PAS à votre Code de secours. Votre Code de secours ne peut jamais être recréé et n'est JAMAIS stocké dans votre application SQRL. Autrement dit, vous ne devez JAMAIS perdre le Code de secours de votre identité. Il ne peut pas être récupéré ni remplacé. Et il est disponible et visible UNIQUEMENT lors de la création de l'identité.

Et si mon identité est stockée sur une machine que j'ai l'intention de donner à quelqu'un ?

Votre identité est très fortement chiffrée à l'aide de votre mot de passe et de votre Code de secours. Si votre mot de passe est suffisamment complexe, il ne devrait pas y avoir de problème. Cela dit, il n'y a non plus aucune raison de laisser votre identité sur un ordinateur que vous ne comptez plus utiliser. L'application SQRL pour Windows publiée par GRC sauvegarde l'identité de son utilisateur dans un dossier « SQRL », créé dans le dossier « Documents » dudit utilisateur. Donc, si vous utilisez cette application, cliquez avec le bouton droit sur l'icône de l'application et choisissez l'option « Quittez l'application » dans le menu contextuel. Ensuite, effacer toutes les identités stockées dans le dossier SQRL indiqué plus haut. Vous les reconnaîtrez facilement : elles portent le nom de l'identité suivi de l'extension « .sqrl ». Videz ensuite la Corbeille.

Comme les système Android et iOS se chargent de la gestion des fichiers pour leurs utilisateurs, ces applications intègrent leur propre fonction de destruction d'identité, à trouver dans les options de ces applications.

Et si mon smartphone ou mon disque dur tombe en panne ? Puis-je transférer mon identité vers un autre appareil ?

Le QR code de la version imprimée de votre identité peut contenir ou pas le mot de passe de son utilisateur. Dans le cas où le QR code contient le mot de passe, il vous suffit de scanner le QR code avec l'application SQRL installée sur un autre appareil, ou d'entrer à la main le texte correspondant. Validez par le mot de passe et voilà, l'identité est prête à être utilisée.

Si l'identité dans sa forme papier a été exportée sans contenir le mot de passe (ce qui est une méthode de stockage à long terme plus sécurisée puisqu'elle ne peut donc pas être utilisée sans le Code de secours), vous devrez donc fournir le Code de secours de l'identité, après avoir scanné le QR code ou avoir tapé le texte de l'identité. Le Code de secours est indispensable pour déchiffrer l'identité, pour vous permettre ensuite de lui donner un mot de passe pour son utilisation au quotidien.

Et si la clé USB que j'utilise pour sauvegarder mon identité est illisible ?

C'est la raison pour laquelle nous poussons vraiment tous les utilisateurs à disposer d'une copie imprimée de leur(s) identité(s).

Vous vous rappelez des ordinateurs des années 1970 qui utilisaient des cartes perforées et d'énormes bandes magnétiques ? Si vous ne vous en souvenez pas, faites-nous confiance, ces méthodes ont vraiment existé. Un peu plus tard, on enregistrait des fichiers sur des disquettes de 8 pouces (20 centimètres de diamètre). Elles ont bien sûr disparu également. Mais les ordinateurs ont toujours pu imprimer sur papier. Et c'est la seule méthode qui existe encore aujourd'hui, alors que toutes celles décrites précédemment ont disparu. Autrement dit, le papier n'a rien rien de bien excitant, mais il s'agit pourtant de la méthode de stockage la plus fiable lorsque le volume d'information à stocker est très faible et que l'on n'a pas besoin de récupérer cette information de la manière la plus rapide possible. Et on pourra encore la lire et l'utiliser dans 50 ans.

Mais, répondons tout de même à la question : tous les appareils sur lesquels vous stockez/utilisez votre identité SQRL servent de sauvegarde à tous les autres. Et donc, si vous n'avez pas encore de sortie papier de votre identité, arrêtez de lire maintenant et trouvez une imprimante 🙂.

Et si je décède ou devient frappé(e) d'incapacité ? De quelle manière ma famille ou mon responsable légal vont-ils pouvoir s'occuper de mes affaires ?

Dans ce cas, l'utilisation de SQRL rend justement les choses bien plus simples.

En partant de l'hypothèse que votre décès ou votre incapacité totale laisse intact tout ou partie des appareils sur lesquels est stockée votre identité SQRL, votre Code de secours est suffisant

pour récupérer l'accès à votre identité et l'utiliser en ligne. À condition naturellement que votre smartphone ou ordinateur soit accessible, c'est-à-dire déverrouillage par vos proches.

Si vos appareils sont inaccessibles, vos proches ou responsables légaux auront besoin d'avoir à la fois accès à une version sauvegardée de votre identité (papier ou autre) et à votre Code de secours.

Dans les deux cas, au moins votre Code de secours (mais de manière plus sûre encore, votre identité et votre Code de secours), devrait être stocké avec vos autres documents officiels/légaux, le tout conservé par votre avocat ou dans un coffre, pour être accessible au moment de votre décès ou de votre incapacité légale.

Puisque le Code de secours peut être utilisé pour modifier le mot de passe de votre identité si vous l'avez oublié, vous pouvez donc le changer quand bon vous semble, sans influence sur les documents stockés chez votre avocat. Mais si vous réencryptez votre identité SQRL, il faudra alors imprimer votre identité de nouveau, avec son nouveau Code de secours, pour la confier de nouveau à votre représentant légal.

Et si mes parents décèdent ? Comment puis-ja avoir accès à leurs différents comptes en ligne protégés par leur identité SQRL ?

La réponse à cette question est similaire à celle de la question précédente. Pour récupérer un accès total à une identité SQRL, il faut disposer à la fois de l'identité et de son Code de secours. Autrement, lorsque vos parents atteignent un âge avancé ou qu'ils deviennent moins autonomes, ils devraient tous deux imprimer leur identité SQRL et leur Code de secours pour les placer dans une enveloppes fermée, et confier cette enveloppe à leur personne de confiance.

Et si je perds absolument tout ? Tous mes appareils, toutes mes impressions, toutes mes sauvegarde ?

Il n'y a rien de mieux que le papier, ni de plus sécurisé ou facile à gérer. Mais une identité SQRL peut AUSSI être exportée sous la firme d'un fichier informatique de très petite taille. Et son Code de secours peut être sauvegardé dans un petit fichier texte. Ces deux fichiers peuvent ensuite être regroupés dans une archive au format Zip, elle-même protégée par un mot de passe. Cette archive Zip peut ensuite être transférée vers n'importe quel service de sauvegarde en ligne.

NOTEZ CELA DIT QUE NOUS NE RECOMMANDONS AUCUNE DE CES MÉTHODES ! Car cela réduit énormément le niveau de sécurité de votre identité SQRL. Mais il s'agit de la seule réponse possible à cette question, car la perte de tous ces éléments permettant d'accéder à votre identité SQRL serait effectivement très gênante (et c'est un euphémisme).

N'oubliez pas non plus que dans ce scénario catastrophe, vous n'auriez pas accès non plus à votre service de stockage en ligne si jamais il était protégé par votre identité SQRL. Il faudrait alors conserver un accès traditionnel par identifiant et mot de passe, ce qui n'est pas le but.

Donc, oui, les différentes méthodes de sécurisation de votre identité SQRL peuvent être stockées de manière sécurisée en dehors de chez vous. Et cela peut d'ailleurs s'avérer être une meilleure solution pour « notariser » votre identité SQRL et la rendre disponible si vous disparaissez ou que vous devenez incapable de l'utiliser : créez le fichier Zip décrit plus haut et un compte de

stockage en ligne gratuit pour l'y stocker. Partagez le tout avec une personne de confiance. Et il vous suffira de mettre à jour ce fichier Zip en cas de réencryption de votre identité.

Et si je veux m'authentifier sur un site Web qui n'utilise pas SQRL?

Ce sera vrai pour tous les sites Web au moment du lancement de SQRL. Nous ne pouvons que vous suggérer de prendre le temps de proposer aux sites Web que vous utilisez d'intégrer SQRL et éventuellement de leur fournir des liens vers des ressources leur expliquant de quoi il s'agit, comme par exemple sqrl.grc.com, au moins au début. Et de recommencer quelques mois plus tard si aucun changement n'a eu lieu.

Et si je ne veux pas utiliser de mot de passe avec mon identité SQRL?

Le mot de passe de SQRL est habituellement utilisé pour décrypter et déverrouiller votre identité SQRL lorsque vous en avez besoin. Le but étant d'éviter que quelqu'un d'autre que vous puisse utiliser votre application SQRL sans que vous le sachiez et donc d'éviter que quelqu'un puisse se faire passer pour vous.

Cela dit, lorsque l'application SQRL est installée sur un appareil offrant des outils de sécurisation alternatifs, comme un capteur d'empreinte digitale ou de reconnaissance faciale, il est possible d'utiliser ces derniers après avoir entré une première fois le mot de passe pour décrypter l'identité. Ensuite, pour chaque authentification sur un site Web, l'empreinte digitale, la reconnaissance faciale ou autre est suffisante pour valider la connexion à chaque site Web que vous visitez.

Et si j'essaie de me connecter à Amazon mais que le message de confirmation indique « Amaz0n »?

Si l'application SQRL qui vous sert à vous identifier est installée sur le même appareil que celui utilisé par le navigateur Internet utilisé pour visiter le site Web, le système SQRL vous protège automatiquement de tout type de tentative de *spoofing* (usurpation d'identité), de faute de frappe ou de piratage. Mais ces fonctions de protection ne sont pas opérantes lorsque vous utilisez votre smartphone pour vous authentifier sur un site ouvert dans le navigateur de votre ordinateur. C'est la raison pour laquelle il est beaucoup plus sécurisé d'utiliser l'application installée sur le même appareil que celui utilisé pour visiter un site Web.

Lorsque l'on utilise un application SQRL pour scanner un QR code, les fonctions de protection anti-spoofing, anti-faute de frappe et anti-piratage ne sont pas disponibles. C'est pourquoi bien vérifier visuellement que l'application vous propose bien de vous authentifier sur le bon site Web est ENTIÈREMENT de votre responsabilité. Toutes les applications SQRL développées dans les règles vous aideront à vérifier que le site sur lequel vous êtes sur le point de vous connecter est bien le bon et vous demanderont une confirmation explicite.

Dans le cas décrit dans la question, vous « authentifieriez » votre identité auprès d'un faux-site Amazon portant le nom de « Amaz0n ». Cela n'est pas très grave en soi, mais cela indique que probablement vous n'êtes pas là où vous souhaitez être. Autrement dit, il vaut certainement mieux ne PAS valider l'authentification. Dans cet exemple, il vaudrait mieux prendre le temps de bien

retaper lentement l'adresse « amazon.com » dans la barre d'adresse de votre navigateur. Et prenez VRAIMENT le temps de détailler la question suivante et sa réponse, car il s'agit d'un sujet CRUCIAL !

Et si je me connecte à « voyou.com » mais que le message de confirmation affiche « amazon.com » ?

Comme il est expliqué dans la question précédente, si vous n'utilisez PAS le QR code pour vous authentifier sur un site en utilisant l'application SQRL installée sur un autre appareil, SQRL vous protège automatiquement de ce type de tentative de spoofing (usurpation de nom de site Web), de faute de frappe ou de piratage. Mais ces fonctions de protection ne sont pas opérantes si vous scannez un QR code SQRL depuis un autre appareil que celui sur lequel vous visitez le site Web.

C'est pourquoi, lorsque vous scanner un QR code d'authentification depuis une application SQRL installée sur un smartphone, le danger réside dans le fait que le site « voyou.com » espère que ses visiteurs ne fassent pas attention et qu'ils s'authentifient sur « amazon.com » sans regarder. La procédure utilisée par le site « voyou.com » est la suivante. Il commence par attendre que quelqu'un commence à s'y authentifier. Le site commence alors en arrière-plan un processus d'authentification sur Amazon pour en obtenir le QR code. Le site « voyou.com » vous présente ensuite le QR code d'Amazon. Du coup, si l'utilisateur ne fait pas attention, il confirme son authentification sur Amazon plutôt que sur « voyou.com », donnant alors à ce dernier accès à son compte Amazon.

Lorsque l'on utilise une application SQRL sur le même appareil que celui utilisé pour visiter le site sur lequel on visite le site Web auquel on veut se connecter, SQRL vous protège complètement contre ces attaques en vérifiant pour vous la provenance de la demande d'authentification (autrement dit qu'il s'agit bien du même site Web). Mais il n'y a malheureusement aucune façon de réaliser cette opération si vous utilisez une application SQRL sur votre smartphone pour scanner le QR code qui s'affiche dans le navigateur de votre ordinateur. Dans ce cas, c'est à l'utilisateur qu'incombe la responsabilité de vérifier qu'il s'identifie bien sur le bon site.

Et si je veux me connecter sur amazon.com, mais que je tape « anazon.com » sans m'en rendre compte ?

Comme pour tous les problèmes du même genre, vous êtes totalement protégé de ce genre de danger si vous utilisez l'application SQRL installée sur le même appareil que celui sur lequel vous visitez le site Web (voir les deux explications détaillées précédentes). Mais si vous scannez le QR code d'un site sur votre ordi à l'aide de votre smartphone, alors, il faut être un peu plus prudent.

Et il s'agit alors du pire problème possible de piratage de nom de site Web, puisque vous êtes persuadé que vous allez vous connecter sur le site que vous souhaitez, alors qu'il s'agit d'un site « faute de frappe ». Du coup, lorsque votre smartphone vous demande de confirmer que vous voulez effectivement vous connecter sur « www.amazon.com », vous aurez tendance à approuver sans coup férir, alors même que vous n'êtes PAS sur le site d'Amazon et que vous avez donc été réellement trompé.

Le fait que cette attaque fonctionne aussi bien et aussi automatiquement n'est pas une faiblesse de SQRL uniquement. Si vous avez mal tapé l'adresse du site Web sur lequel vous souhaitez vous

rendre, ici Amazon, vous vous retrouveriez donc à donner vos identifiant et mot de passe à un autre site se faisant passer pour Amazon. Cela dit, la situation est pire dans un monde sans SQRL car, dans ce cas, vous donnez alors au faux site les vrais identifiant et mot de passe de votre compte Amazon. Avec SQRL au moins, cela ne fonctionne qu'une seule fois, mais cela rend l'erreur plus facile à faire et plus automatique.

Autrement dit, comme expliqué dans les deux dernières questions, lorsque vous utilisez SQRL avec un QR code, vous acceptez un niveau de sécurité un peu moindre en échange d'une procédure légèrement plus simple en optant pour une authentification « à distance ». Soyez vraiment prudent !

Et si une personne d'un service technique me demande mon mot de passe SQRL ?

Vous ne devez JAMAIS donner votre mot de passe SQRL à quiconque. Ce n'est pas un mot de passe de site Web comme les autres. Il ne peut être utilisé que pour décrypter et déverrouiller votre identité SQRL personnelle et personne d'autre que vous n'a de raison valable de l'obtenir et de s'en servir.

Tout au plus, une personne qui vous aide pour un problème technique peut vous demander de vérifier que vous êtes bien la personne que vous prétendez être en vous demandant de vous rendre sur un site Web particulier et de vous y authentifier à l'aide de votre application SQRL. Il n'y aucune raison d'aller au-delà.

Et si un site Web se fait pirater et voler sa base de données utilisateurs, que se passe-t-il ?

Rien. Votre identité SQRL n'est concernée en rien, ni aucunement mise en danger puisque le système SQRL ne demande à aucun site Web de stocker quelque information secrète que ce soit.

Les sites Web qui utilisent les traditionnels (et dépassés !) identifiants et mots de passe doivent les garder secrets puisqu'il s'agit de leur seul moyen de s'assurer de l'identité de leurs visiteurs. Du coup, lorsqu'un site se fait pirater, il doit en informer tous ses utilisateurs et leur conseiller de changer leur mot de passe et aussi de ne jamais réutiliser celui qu'ils viennent de se faire voler sur un autre site.

Rien de tout ça ne s'applique à SQRL.

Avec SQRL, les sites Web n'ont rien de secret à conserver, donc ils n'ont rien à perdre.

Et si j'ai un doute sur une application SQRL ?

Toutes les applications SQRL ont la responsabilité de s'assurer et de protéger l'identité de son utilisateur en ligne. Ce qui signifie que les utilisateurs doivent avoir absolument confiance dans leur application SQRL. Cette dernière doit donc être conçue et programmée dans les règles. Mais comme les utilisateurs non informaticiens n'ont aucun moyen de s'en assurer, ils ne peuvent que s'appuyer sur l'opinion de ceux qui savent le faire. Autrement dit, les utilisateurs de SQRL doivent s'appuyer sur la réputation et l'historique des applications SQRL qu'ils souhaitent utiliser.

PERSONNE ne devrait télécharger, faire confiance ni utiliser une application SQRL trouvée au hasard. Rien de mieux pour se retrouver en difficulté. La plupart des applications SQRL sont développées et distribuées en open source ce qui permet à la communauté des développeurs bienveillants d'en étudier, vérifier et améliorer le code source. Naturellement, cela signifie que les pirates y ont également accès et qu'ils peuvent détourner le code pour le transformer en arme contre vous.

En d'autres termes, il n'y aurait rien de plus facile que de créer une application SQRL malveillante, capable de vous voler votre identité, et c'est une quasi certitude que cela se produira. Heureusement, les utilisateurs SQRL n'ont pas besoin d'une panoplie complète d'applications. Une application par type d'appareil suffit. Au moment du lancement de SQRL, il en existait déjà des versions auxquelles on peut faire confiance pour tous les types d'appareils. Utilisez donc celles qui sont recommandées sur le forum SQRL, et votre identité SQRL restera pleinement en sécurité.

Et si le site sur lequel j'utilise SQRL change d'adresse URL ?

Cela sera géré de manière transparente par le site Web et ne gênera en rien votre utilisation de SQRL.

Les sites Web ont la possibilité de transférer leurs utilisateurs SQRL vers un nouveau nom de domaine, au moment de leur première connexion auprès de ce nouveau nom de domaine. Et même si cela ne fonctionne pas, le site aurait tout de même obtenu la clé SQRL de leur utilisateur pour le nouveau domaine. Le site Web peut alors présenter une nouvelle page avec un nouveau bouton « Se connecter avec SQRL » et un nouveau QR code. Une fois l'authentification réussie, le site Web détiendra la clé d'identification SQRL spécifique de l'utilisateur pour l'ancienne et la nouvelle adresse du site. Il ne reste plus au site Web qu'à remplacer l'ancienne clé SQRL par la nouvelle. Les authentifications suivantes se passeront sans problème, comme si l'ancien site n'avait jamais existé.

Et si je ne veux plus utiliser SQRL avec un site en particulier ?

Pour éviter tout problème, les clés SQRL sont liées de manière immuable à leur site Web une fois qu'elles ont été enregistrées pour la première fois. Pour éviter qu'un voleur qui aurait d'une façon ou d'une autre obtenu l'accès à votre identité SQRL et à votre mot de passe de remplacer votre identité par la sienne, seul votre Code de secours peut être utilisé pour modifier ou effacer la clé SQRL liée à un site Web. Mais si vous possédez votre Code de secours, il n'y a rien de plus simple. Au moment de l'authentification, cliquez sur le bouton Options, puis sélectionnez « Effacer ou Remplacer l'identité SQRL », tapez votre Code de secours et continuez la procédure d'identification. Le site Web obtiendra l'information que vous souhaitez changer ou effacer votre identité SQRL et fera ce que vous lui demandez.

Et si je veux uniquement utiliser SQRL comme méthode d'identification sur un site Web ?

Dans le domaine de la sécurité, comme dans le cas de la résistance d'une chaîne, la résistance du maillon faible détermine la résistance de l'ensemble. Même dans un monde disposant des

techniques super sécurisée de SQRL, un pirate peut toujours parvenir à vous voler vos identifiants et mots de passe.

Pour résoudre ce problème, les applications SQRL proposent toutes une options appelée « Request SQRL-only sign in » (Demander de n'accepter que les authentifications SQRL) et « Request no account recovery » (Demander de n'accepter aucune demande de récupération de compte). Ce sont des demandes auxquelles n'importe quel site Web peut répondre mais que SQRL ne peut rendre obligatoires. Cela dit, les utilisateurs SQRL peuvent vérifier si ces demandes sont honorées tout simplement en tentant de s'identifier auprès d'un site Web à l'aide de leur ancien mot de passe.

Ces demandes sont mémorisées par l'application SQRL et envoyées au site Web à chaque authentification. Donc, dès qu'un utilisateur SQRL se sent à l'aise avec le système SQRL (et que leur identité et Code de secours sont bien stockés en sécurité quelque part, il peut alors activer ces options pour que les sites n'acceptent plus que leur authentification SQRL et éviter ainsi toute attaque « traditionnelle » contre leur identification sur les sites Web compatibles SQRL.

Les trois règles d'or de SQRL

Les trois règles d'or pour une utilisation sécurisée de SQRL

1- Faites une sauvegarde de votre identité SQRL et de votre Code de secours et stockez-les dans un endroit sûr

Au fur et à mesure de l'adoption de SQRL par les sites Web, l'importance de votre identité SQRL grandira. À partir du moment où vous aurez sauvegardé comme il faut votre identité SQRL et son Code de secours une fois, vous serez paré à toute éventualité. Donc, faites-le une fois. Et faites-le maintenant.

2- N'utilisez JAMAIS une application SQRL dans laquelle vous n'avez pas confiance. Utilisez UNIQUEMENT des applications de confiance

Toutes les applications SQRL ont la responsabilité de s'assurer et de protéger l'identité de son utilisateur en ligne. Ce qui signifie que les utilisateurs doivent avoir absolument confiance dans leur application SQRL. Cette dernière doit donc être conçue et programmée dans les règles. Il ne fait aucun doute que des pirates tenteront de voler des indemnités SQRL en proposant des application SQRL malveillantes, se faisant passer pour des applications de confiance. Les

applications proposées sur ce forum ont été développées par des personnes ayant de bonnes intentions. Si nous leur faisons confiance, vous pouvez leur faire confiance aussi.

3- Vérifiez TOUJOURS l'adresse du site Web auquel vous vous connectez à l'aide de SQRL

Vous êtes totalement protégé de ce genre de danger si vous utilisez l'application SQRL installée sur le même appareil que celui sur lequel vous visitez le site Web. Mais si vous scannez le QR code d'un site sur votre ordi à l'aide de votre smartphone, alors, il faut être un peu plus prudent. Il est en effet possible qu'un site Web malveillant affiche un QR code lié à un site différent de celui auquel vous souhaitez vous connecter. Et si le faux nom est proche de celui que vous souhaitez, vous ne le remarquerez peut-être pas si vous n'y prêtez pas suffisamment attention. Donc,; si vous utilisez votre smartphone pour scanner un QR code, soyez DOUBLEMENT PRUDENT dans la vérification de l'adresse du site sur lequel vous souhaitez vous authentifiez.