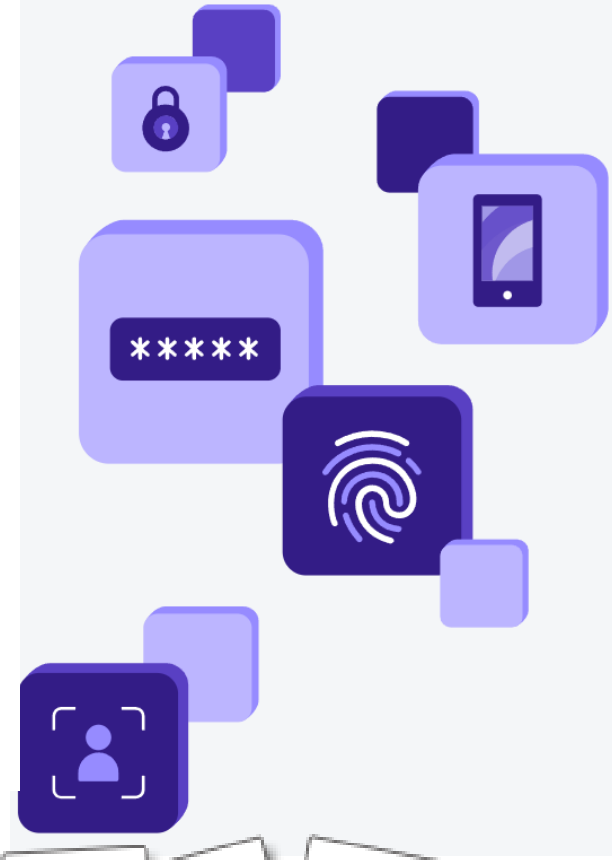
TUTOS-INFO
L'informatique par l'exemple

2FA

Connect. Protect.



SOMMAIRE

Sources : Le Journal du Coin – Coin Academy - Streammind

https://tutos-info.fr

1 - DEFINITION DU « 2FA »

L'authentification à deux facteurs souvent appelée « 2FA » est le processus d'authentification où deux des trois facteurs possibles d'authentification sont combinés.

Les facteurs possibles d'authentification sont :

- quelque chose que l'utilisateur connaît : un mot de passe, un numéro d'identification personnel (code PIN) ou une réponse à une question secrète
- quelque chose que l'utilisateur a : par exemple un jeton, un téléphone mobile, un USB, un porte-clés
- quelque chose que l'utilisateur est : par exemple la reconnaissance faciale ou vocale, la biométrie comportementale, l'empreinte digitale, la rétine ou l'iris

Dans le cas de la sécurité Internet, les facteurs d'authentification les plus utilisés sont : quelque chose que l'utilisateur possède (par exemple une carte bancaire) et quelque chose que l'utilisateur sait (par exemple un code PIN). Il s'agit **d'authentification à deux facteurs**. L'authentification à deux facteurs est aussi parfois appelée authentification forte, vérification en deux étapes ou **2FA**.

La principale différence entre l'authentification multifactorite (AMF) et l'authentification à deux facteurs (2FA) est que, comme le terme l'indique, l'authentification à deux facteurs utilise une combinaison de deux facteurs d'authentification, tandis que l'authentification multifactorite (AMF) pourrait utiliser deux ou plusieurs de ces facteurs d'authentification.

2 - FONCTIONNEMENT DU « 2FA »

Lorsque vous vous connectez à votre plateforme, vous serez invité à vous authentifier avec votre nom d'utilisateur et votre mot de passe. Cela devient votre premier facteur d'authentification.

Pour le deuxième facteur d'authentification, vous pouvez utiliser :

- un code de vérification envoyé sur votre mobile par SMS
- un « authentificateur » spécialisé comme Google Authenticator.

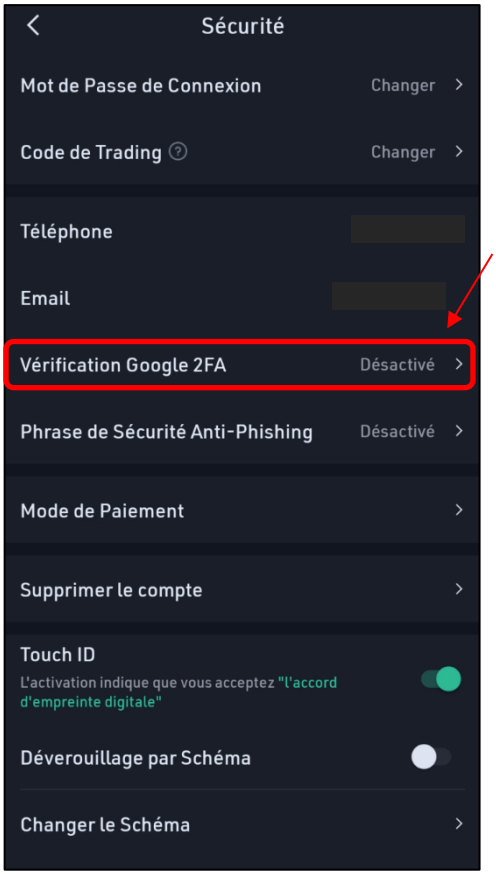
La combinaison avec votre nom d'utilisateur et mot de passe, applique une couche supplémentaire de sécurité plus forte et plus résiliente.

Parce que la méthode d'authentification simple avec mot de passe n'est plus suffisante de nos jours pour arrêter les attaques, l'authentification à deux facteurs fournit une couche secondaire de sécurité qui rendra la tâche plus difficile pour les pirates.

Vous devez utiliser l'authentification à deux facteurs pour :

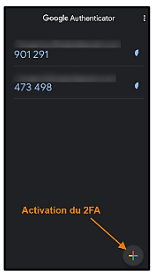
- les services bancaires en ligne
- les achats en ligne (Amazon, PayPal, Google Play)
- les plateformes d'échange de crypto monnaies

3 - MISE EN PLACE DU « 2FA » AVEC GOOGLE AUTHENTICATOR



✓ Commencez, dans un premier temps, par télécharger sur votre mobile le « Google Authenticator » (vous le trouverez dans le store) et connectez Google Authenticator à votre compte Gmail par exemple.

✓ Ouvrez votre application mobile et recherchez, dans les paramètres, la rubrique « SECURITE ». Vous trouverez, dans cette rubrique, l'option permettant d'activer le 2 FA.



✓ Activez le 2FA depuis l'application : un QR CODE s'affiche
✓ Lancez votre « Google Authenticator »
✓ Cliquez le « + » en bas à droite de l'écran du Google Authenticator

✓ Scannez le QR CODE fourni par l'application
✓ Votre application est maintenant liée au Google Authenticator

A chaque fois que vous vous connecterez à votre application mobile, vous devrez, en plus d'effectuer la saisie de vos identifiants, saisir le code fourni par Google Authenticator (2 facteurs).

Attention, cette protection n'est malheureusement pas disponible sur tous les sites. Son utilisation est parfois obligatoire pour accéder à toutes les fonctionnalités d'une plateforme.

> ⚠ **Attention**, un code de récupération vous est donné avec le QR Code (2FA backup key). Notez-le quelque part et gardez-le bien précieusement **en lieu sûr**. N'hésitez pas à en faire plusieurs copies physiques. Il s'agit d'un code de secours nécessaire pour récupérer votre compte si vous perdez votre smartphone et donc, votre accès à Google Authenticator.

Lorsque vous utilisez Google Authenticator, un code s'affiche dans le Google Authenticator : ce code (6 chiffres) a une durée de vie très limitée (30 secondes) et vous devez le copier-coller dans votre application mobile pour valider votre authentification (le nom de l'application qui est liée est affichée au-dessus du code aléatoire) :

Code à 6 chiffres généré par Google Authenticator que vous devez coller dans votre appli mobile (un appui long sur le code permet de le copier en mémoire).

Le code généré par Google Authenticator a une durée de vie limitée (30 sec). Une fois le décompte terminé, un nouveau code sera

LE « SIM SWAP » QUI PERMET DE CONTOURNER LE 2FA FRAPPE AUSSI LA CRYPTOSPHÈRE

Cryptomonnaies & Altcoins | Scams

07 août 2018 à 12h00 par Grégory Guittard

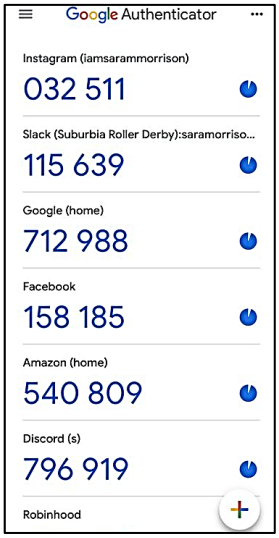
QUEL A ÉTÉ SON MODE OPÉRATOIRE ?

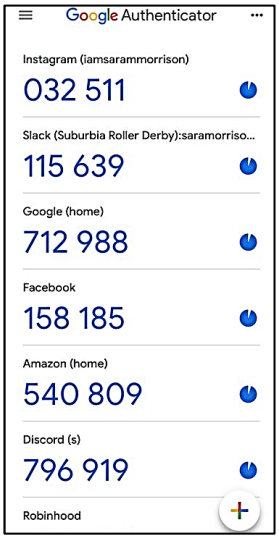
En l'état, Joel Ortiz, aidé par des complices non nommés, aurait ciblé une partie des crypto-investisseurs s'étant rendus à la conférence Consensus. En obtenant leurs coordonnées téléphoniques, il aurait alors pu se faire passer pour ses victimes auprès de leurs opérateurs téléphoniques respectifs, afin de demander le transfert de leurs lignes vers des cartes SIM qu'il possédait. **40 victimes sont à l'heure actuelle recensées**. Et le tour était joué : quand les victimes se sont rendues compte de la supercherie, avec la désactivation de leur ligne suite au swap, il était déjà trop tard pour agir. Gagnant l'accès aux divers comptes relatifs aux réseaux sociaux et aux plateformes d'échange crypto utilisés par ses victimes, **Joel Ortiz a réussi avec ses complices à détourner près de 5 millions de dollars de cryptomonnaies diverses.**

La protection par mots de passe a vécu

Tout est parti d'un constat : le système des mots de passe a vécu. Il présente trop de faiblesses pour offrir une sécurité absolue.

- En premier lieu, un grand nombre d'utilisateurs se servent d'expressions que les hackers peuvent « craquer » aisément. Chaque année, Splashdata publie la liste des 25 mots de passe les plus utilisés. On peut avoir du mal à y croire mais la réalité est là, le n° 1 du lot est : « 123456 ». Le n° 2 est à peine plus complexe : « 123456789 ». Et le n° 3 est « QWERTY », ce qui correspond aux six premières lettres d'un clavier américain.
- Il est également courant que des usagers utilisent des combinaisons aisées à deviner. Exemple : Claude Dubois, né le 24 janvier 1984, va avoir pour mot de passe : « CD240184 ».
- Quand bien même le mot de passe serait plus complexe, les hackers ont développé un grand nombre de techniques pour amener un utilisateur à dévoiler malgré lui son mot de passe. L'une de ces méthodes est le *phishing*, soit un site qui reproduit fidèlement l'interface d'un site connu comme Amazon.
- Une autre méthode consiste à placer sur l'ordinateur d'un usager un *keylogger*, c'est-à-dire un programme qui enregistre ce qu'il tape sur son clavier.
- Il est courant que des bases de données soient piratées et que des hackers accèdent ainsi aux mots de passe de très nombreux usagers. En septembre 2018, Facebook a été contraint de révéler qu'une faille de sécurité avait ainsi compromis 50 millions de comptes, dont 200.000 sur la France.





La nécessité d'alternatives aux mots de passe

Pour remédier aux faiblesses du système des mots de passe, maints systèmes ont été imaginés.

- Si vous avez un iPhone, vous savez qu'Apple a opté, depuis quelques années déjà, pour une identification biométrique (la reconnaissance d'attributs physiques) comme sésame de votre appareil. Tout d'abord les empreintes digitales, plus récemment, l'identification du visage.
- Des applications tels que Dashlane, 1Password, KeePass ou LastPass créent des mots de passe ultracomplexes et différents pour chaque site visité, et les fournissent d'eux-mêmes à chaque visite.
- Des systèmes de protection impliquant une clé USB ont été mis au point, tels la Yubikey de Yubico. Dans le secteur des cryptomonnaies, la société française Ledger propose une clé de ce type, qui stocke tous les accès aux *wallets* (portefeuilles) et *exchanges* (places de marché).
- Des sociétés telles que Google ou Microsoft planchent, en partenariat avec des sociétés telles que Visa ou Mastercard, sur une alternative universelle qui servirait sur le Web.

Toutefois, l'authentification à deux facteurs est le système le plus simple. Il a été mis en place par un grand nombre d'acteurs du Web, notamment les banques et pour cause : la deuxième Directive européenne sur les services de paiement, en vigueur depuis le 13 janvier 2018 - et visant à renforcer la sécurité des paiements en ligne - préconise l'emploi de cette authentification à deux facteurs par les prestataires de services de paiement.