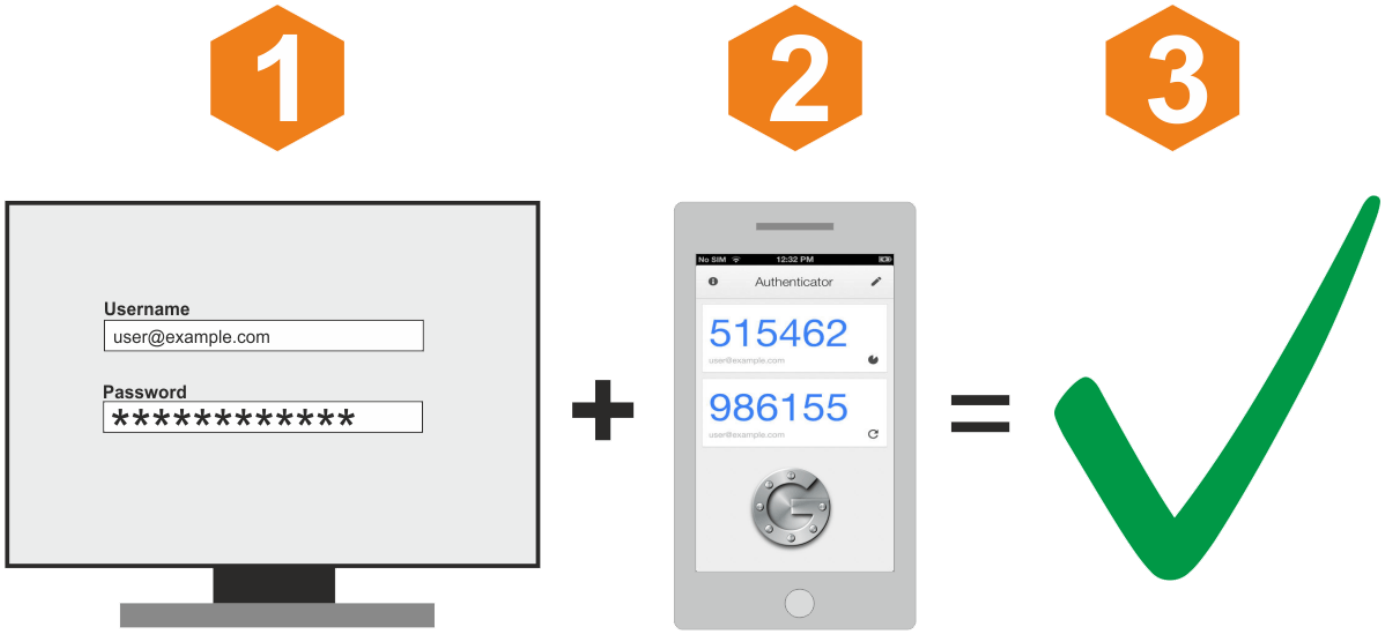
www.howtogeek.com /117047/why-you-should-use-two-factor-authentication-2fa/

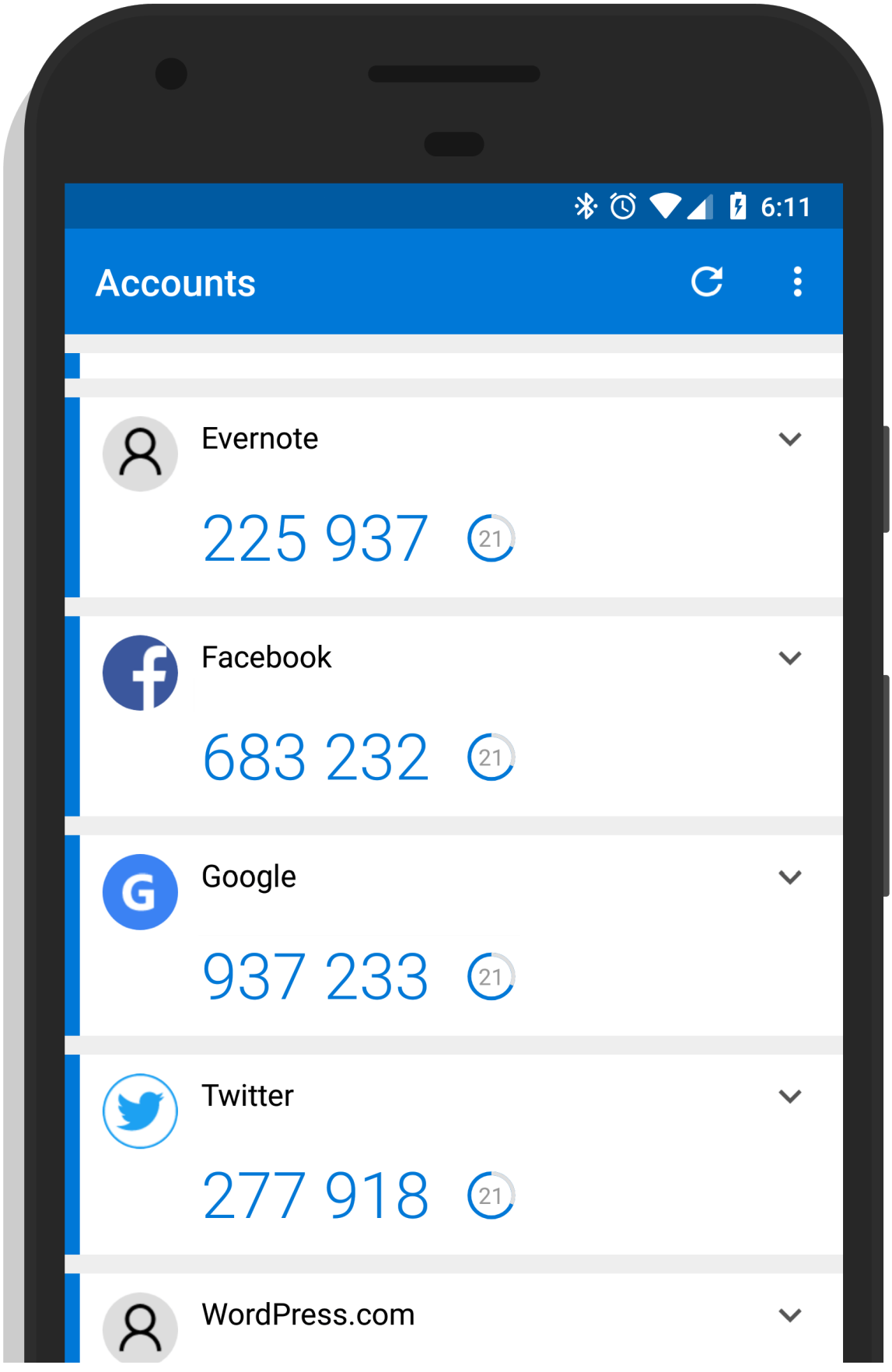
Voici pourquoi vous devriez utiliser l’authentification à deux facteurs (2FA)

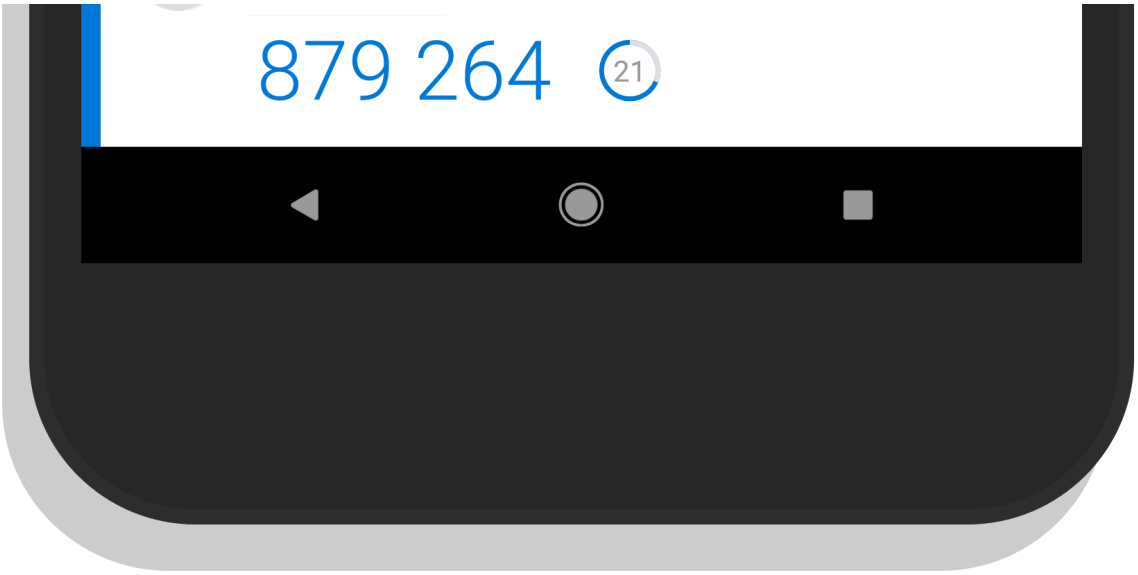
Si vous avez reporté l’utilisation de 2FA, aujourd’hui est le jour idéal pour prendre au sérieux la sécurité

Jason Fitzpatrick :

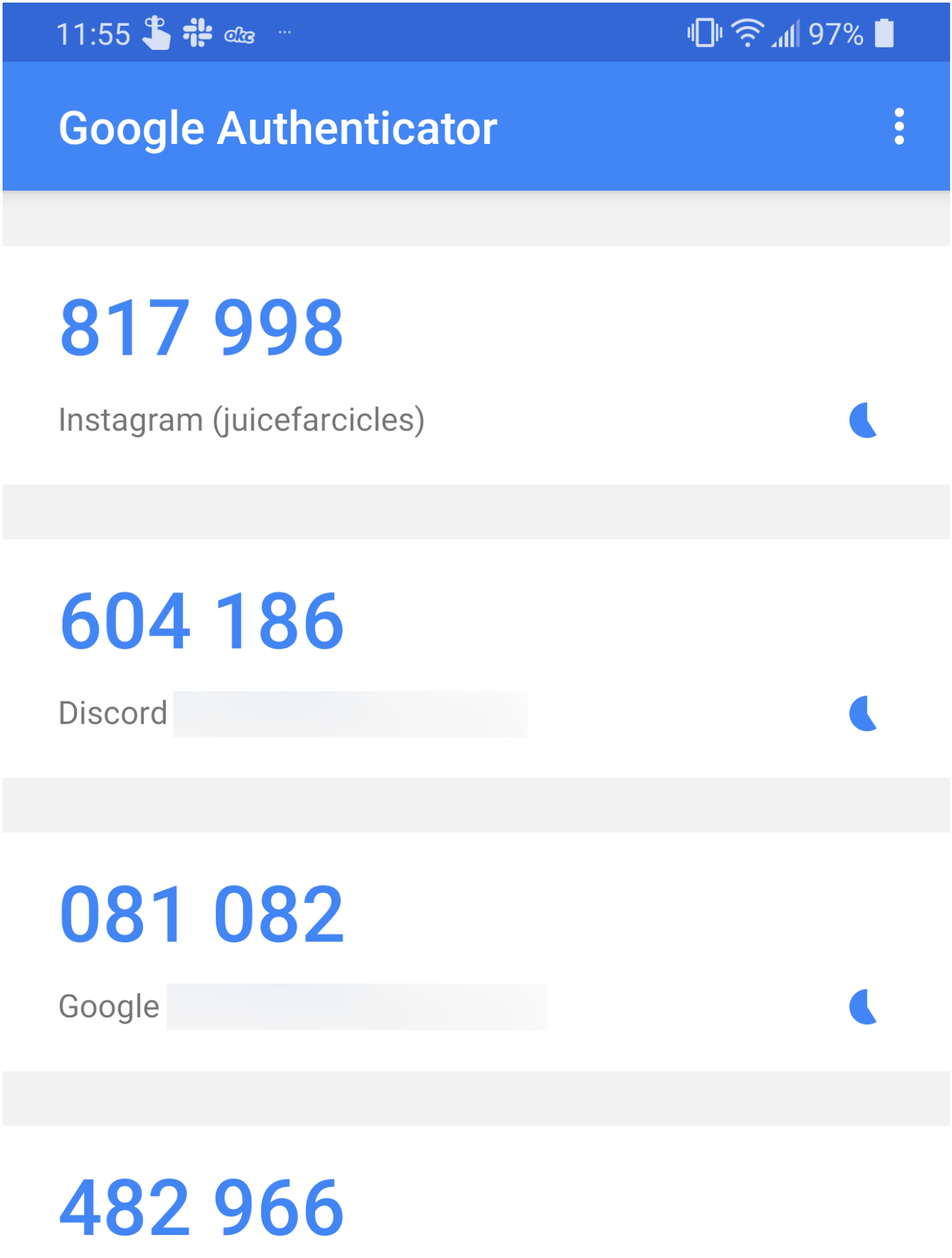


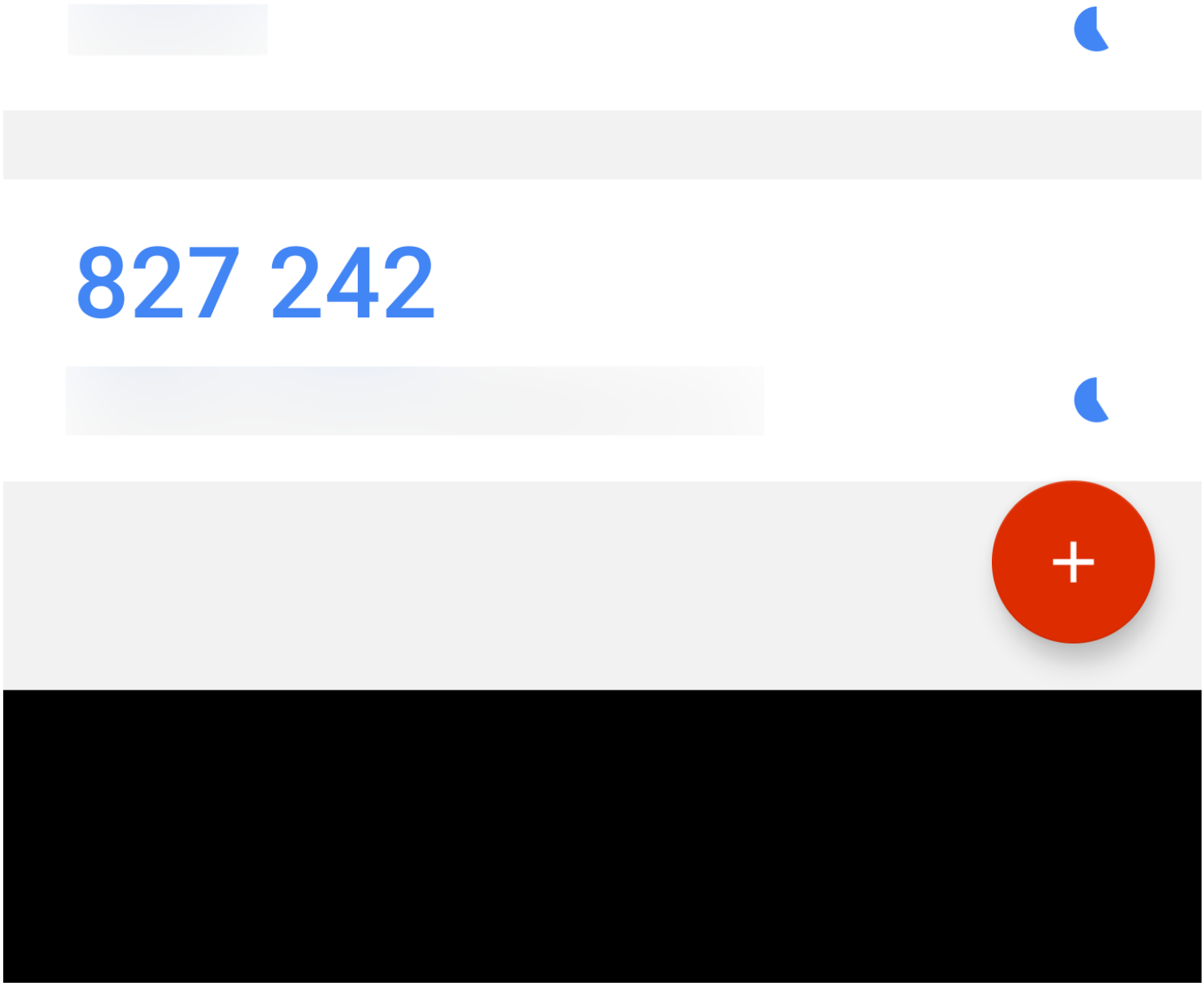
Microsoft Authenticator


6:11
Accounts
Evernote
225 937
21
Facebook
683 232
21
Google
937 233
21
Twitter
277 918
21
WordPress.com



Google Authenticator


11:55
97%
Google Authenticator
817 998
Instagram (juicefarcicles)
604 186
Discord
081 082
Google
482 966



Liens rapides

Principaux points à retenir

L’authentification à deux facteurs (2FA) est une mesure de sécurité qui vous oblige à fournir un facteur d’identification supplémentaire (tel qu’un code envoyé à votre téléphone) en plus de votre nom d’utilisateur et de votre mot de passe habituels.

Votre banque, votre fournisseur de messagerie et peut-être même votre plate-forme de jeu préférée vous ont incité à configurer une authentification à deux facteurs.
Si vous ne savez pas ce que c’est ou pourquoi vous souhaitez commencer à l’utiliser, lisez la suite pour savoir comment l’authentification à deux facteurs peut tout protéger, de votre compte bancaire à votre collection de jeux.

Qu’est-ce que l’authentification à deux facteurs ?

Pour comprendre ce qu’est l’authentification à deux facteurs (2FA), examinons d’abord ce qu’est l’authentification à un facteur et comparons-la aux modèles de sécurité réels et virtuels.

Lorsque vous rentrez du travail, sortez vos clés et déverrouillez votre porte, vous utilisez une authentification simple à un facteur.
La porte et l’ensemble de la serrure ne se soucient pas de savoir si la personne qui tient la clé est vous, votre voisin ou un criminel qui a soulevé vos clés.

La seule chose dont la serrure se soucie, c’est que la clé s’adapte ---vous n’avez pas besoin de deux clés, d’une clé et d’une empreinte digitale, ou de toute autre combinaison de contrôles.
La clé physique unique est la seule autorisation, et son détenteur, légitime ou non, obtient un accès complet.

Le même niveau d’authentification à un facteur se produit lorsque vous vous connectez à un site Web ou à un service qui nécessite uniquement votre nom d’utilisateur et votre mot de passe.
Vous, votre conjoint ou toute autre personne pouvez taper le nom d’utilisateur et le mot de passe pour accéder à votre compte, tout comme n’importe qui pourrait prendre la clé de votre maison et ouvrir votre porte.

Vous êtes en bonne forme si personne ne vole jamais vos clés ou votre mot de passe. Alors que le vol de vos clés est un risque assez faible, la sécurité virtuelle est plus complexe.
Les failles de sécurité, les attaques sophistiquées et d’autres aspects malheureux mais trop réels du travail et du jeu dans un espace virtuel nécessitent des pratiques de sécurité améliorées, y compris des mots de passe complexes multiples et diversifiés et, lorsqu’ils sont disponibles, une authentification à deux facteurs.

Qu’est-ce que l’authentification à deux facteurs et à quoi ressemble-t-elle pour vous, l’utilisateur final ?
L’authentification à deux facteurs est un sous-ensemble de l’authentification multifacteur (MFA).
Toutes les authentifications à deux facteurs sont des authentifications multifacteurs, mais toutes les authentifications multifacteurs ne sont pas à deux facteurs (car un système MFA peut nécessiter 3, 4 ou plusieurs facteurs d’authentification supplémentaires). Familièrement, les gens utilisent encore le terme 2FA pour désigner les systèmes multi-facteurs en général, et comme il reste l’implémentation la plus courante de l’authentification multifacteur, nous utiliserons le terme tout au long de cet article.

Au minimum, l’authentification à deux facteurs nécessite deux variables d’authentification sur trois, telles que :

- Quelque chose que vous connaissez (comme le code PIN sur votre carte bancaire ou le mot de passe de votre courriel).
- Quelque chose que vous avez (la carte bancaire physique ou un jeton d’authentification).
- Quelque chose que vous êtes (biométrie comme votre empreinte digitale ou votre motif d’iris).

Si vous avez déjà utilisé une carte de débit, vous avez utilisé une forme simple d’authentification à deux facteurs: il ne suffit pas de connaître le code PIN ou d’avoir physiquement la carte.
Vous devez posséder les deux pour accéder à votre compte bancaire à un guichet automatique.

L’authentification à deux facteurs peut prendre différentes formes tout en répondant à l’exigence 2 sur 3.
Il peut y avoir un jeton physique, tel que les fobs RSA SecurID, qui génère continuellement des codes sécurisés aléatoires pour vous.
D’autres entreprises sautent la route du matériel personnalisé et fournissent des applications de téléphonie mobile (ou des codes envoyés par SMS) qui offrent les mêmes fonctionnalités.

Bien que rare par rapport aux solutions logicielles, vous pouvez également utiliser l’authentification à deux facteurs basée sur la biométrie (comme la sécurisation d’un fichier crypté par mot de passe et empreinte digitale).

En outre, certaines entreprises ont évolué vers un modèle MFA qui inclut les variables d’authentification que vous attendez d’un système 2FA--- comme le besoin d’un mot de passe plus un code à usage unique d’une application d’authentification --- avec l’ajout d’une autre variable, telle que votre emplacement physique ou vos identifiants réseau.

Pourquoi et où dois-je utiliser l’authentification à deux facteurs ?

Nous sommes fermement convaincus que les gens devraient utiliser l’authentification à deux facteurs sur presque tout ce qu’ils utilisent qui offre une authentification à deux facteurs.

C'est un moyen facile et presque sans friction d'accroître la sécurité et de réduire le risque de vol d'identité, de pertes financières et les tracas généraux généraux liés aux violations de sécurité.

Faire un effort conscient pour utiliser des mots de passe aléatoires et forts avec un gestionnaire de mots de passe parallèlement à l'authentification à deux facteurs est une amélioration de sécurité si importante qu'il vaut la peine de brancher un code ou d'authentifier votre identité de temps en temps.
Besoin d'un peu plus de convaincre?
Une analyse Microsoft de 2019 des violations de compte a révélé que 99,9% se produisaient sur des comptes sans 2FA activé.

En avez-vous besoin pour chaque chose?
Pas forcément.
L'authentification à deux facteurs pour un forum de discussion de muscle car que vous utilisez occasionnellement qui ne contient aucune information personnelle et qui n'est pas lié à votre véritable courriel ou à vos informations financières est exagérée.

Une deuxième couche d'authentification pour votre carte de crédit ou votre compte de messagerie principal, cependant, est un excellent renforcement de la sécurité.
Le traumatisme personnel et financier qui résulterait de l'accès d'un voleur d'identité ou d'une autre entité malveillante à ces choses l'emporte de loin sur les tracas mineurs liés à la saisie d'un peu d'information supplémentaire.

Si votre courriel est compromis, cela vous expose à d'autres services qui sont compromis, car le courrier électronique sert en quelque sorte de clé principale pour accéder aux réinitialisations de mot de passe et à d'autres demandes.
(C'est pourquoi nous recommandons aux gens de cesser d'utiliser leur adresse e-mail principale pour se connecter à tout.)

Si votre banque propose une authentification à deux facteurs, profitez-en.
N'oubliez pas les autres outils financiers que vous utilisez comme PayPal.
Si un service peut être utilisé pour envoyer ou recevoir de l'argent ou accéder à vos dossiers financiers, vous devez utiliser 2FA.
Même chose pour tout service qui héberge des éléments personnels tels que des sauvegardes de fichiers, des sauvegardes de photos, etc.

Même pour des choses comme les plates-formes de jeux vidéo, cela en vaut la peine. Non seulement les joueurs passent des centaines d'heures à construire leurs personnages et dépensent souvent de l'argent réel pour acheter des biens dans le jeu, mais perdre tout ce travail et cet équipement est une proposition terrible.

Bien que tous les services n'offrent pas l'authentification à deux facteurs, le nombre d'entreprises offrant un certain type d'authentification à deux facteurs a considérablement augmenté au fil des ans.
Lorsque nous avons commencé à écrire sur 2FA, la liste des organisations et des fournisseurs qui l'offraient était suffisamment courte pour que nous puissions les ébranler dans un paragraphe.

Maintenant, 2FA est relativement courant, et si vous fouillez dans les documents de support ou même simplement dans votre profil et votre page de paramètres sur un service donné, vous trouverez probablement une sorte d'option pour l'authentification à deux facteurs.

Vous pouvez également réduire le temps passé à rechercher en utilisant certains des répertoires 2FA pratiques comme la liste des sites Web 2FA et le répertoire 2FA.
Les deux sites répertorient les services populaires qui prennent en charge 2FA, offrent des informations supplémentaires telles que le type de 2FA qu'ils prennent en charge et des liens vers des documents d'aide pertinents pour chaque service respectif.

Fonctionnement des types courants d'authentification à deux facteurs

Bien que nous ne puissions pas vous montrer exactement comment l'authentification à deux facteurs fonctionnera sur chaque service pour lequel vous l'activez, nous pouvons parler des méthodes 2FA courantes que vous devriez vous attendre à rencontrer et de leur fonctionnement.

Messagerie électronique

Si vous vous êtes déjà connecté à un service et que vous avez été invité à vérifier votre courrier électronique pour un code de vérification, vous avez rencontré une forme très basique d'authentification à deux facteurs.

Nous avons mentionné ci-dessus qu'il est essentiel de sécuriser votre courrier électronique, et c'est pourquoi.
De nombreux services utilisent la vérification de base par courriel et par code.
Si votre courriel est compromis, il en va de même pour tous les services pour lesquels vous utilisez ce courriel.

C’est mieux que rien, mais si vous utilisez un service qui offre autre chose sur cette liste, vous devez l’activer.

SMS et appels vocaux

Semblable à l’envoi d’un code à usage unique, les SMS et les 2FA vocaux envoient le code à votre téléphone par SMS ou en vous appelant et en lisant le code par téléphone.

C’est un système loin d’être parfait car il est vulnérable aux attaques telles que les escroqueries de portage téléphonique, mais c’est mieux que de ne pas avoir 2FA activé du tout.
Si SMS est la seule option 2FA disponible, vous devriez l’utiliser car, imparfaite ou non, il est beaucoup plus difficile pour quelqu’un d’accéder à vos comptes.

Applications d’authentification dédiées

Les applications d’authentification dédiées, qui se concentrent exclusivement sur la génération de codes à usage unique, constituent une avancée significative par rapport aux courriels, SMS ou appels vocaux.

Google Authenticator a été l’une des premières applications d’authentification et reste assez populaire (et la plus grande plainte des utilisateurs, le manque de synchronisation entre appareils, a été corrigée dans le cadre d’une refonte massive de l’application en avril 2023.)
Authy et Duo sont deux autres alternatives remarquables et populaires.

Bien qu’il ne s’agisse pas d’une application 2FA autonome, la populaire application de gestion des mots de passe 1Password dispose d’un authentificateur intégré pour vous aider à gérer vos jetons 2FA.
1Password a également une fonctionnalité intéressante liée à 2FA: il vous avertira si un service que vous avez stocké dans votre coffre-fort de mots de passe prend en charge 2FA et vous aidera à le configurer là-bas.
Si vous recherchez un guichet unique pour une bonne gestion des mots de passe et un déploiement 2FA facile, il est difficile de battre 1Password.

Enfin, il va sans dire que vous n’utilisez que des applications 2FA d’entreprises réputées. Non seulement vous compromettez la sécurité de votre compte en utilisant une application non sécurisée, mais en 2022, il y a même eu un cas d’application d’authentification malveillante installant des logiciels malveillants et volant des informations bancaires.

Notifications d’application mobile

Certains services utiliseront leur application mobile sur votre téléphone comme deuxième forme de vérification d’identité.
Les « invites » de Google sont un exemple de ce type de système 2FA, mais ils ne sont pas la seule entreprise à les utiliser.

Vous pouvez vous connecter au service sur votre ordinateur personnel ou votre ordinateur portable loin de votre réseau domestique, et vous recevrez un message pour ouvrir l’application de l’entreprise sur votre téléphone et confirmer que vous êtes celui qui se connecte à votre compte.

C’est toujours 2FA, il est juste configuré comme une seule livraison de jetons pour un seul fournisseur de services au lieu d’un arrangement de trousseau avec plusieurs jetons dans une application dédiée comme Google Authenticator ou Authy.

Clés 2FA matérielles

Les clés 2FA matérielles sont exactement ce qu’elles sonnent comme---objets physiques que vous utilisez pour authentifier votre identité.
La plupart des clés 2FA physiques sur le marché sont une combinaison de périphériques USB / NFC, vous pouvez donc brancher la clé sur votre ordinateur ou la tenir près d’un smartphone pour l’activer.
Quelques normes existent, mais la plupart des clés 2FA matérielles utilisent la norme FIDO Universal 2nd Factor Authentication (U2F).

Tout comme vous entrez un code à usage unique à partir d’une application d’authentification pour confirmer votre identité, vous pouvez utiliser la clé physique pour faire de même.
Bien que ce soit indéniablement un moyen très cool et sécurisé de faire les choses, la plupart des gens ne suivent pas la voie de la clé matérielle et utilisent leur téléphone et leur application d’authentification comme méthode 2FA plus pratique.

Cependant, vous pouvez utiliser 2FA, c’est le moment idéal pour activer 2FA sur tous les services que vous utilisez et qui le prennent en charge.
Bien que l’authentification à deux facteurs ne soit pas invulnérable aux attaques (une attaque sophistiquée de l’homme du milieu ou

quelqu’un volant votre jeton d’authentification secondaire et vous frappant avec un tuyau pourrait le fissurer), elle est radicalement plus sûre que de s’appuyer sur un mot de passe ordinaire, et le simple fait d’avoir un système à deux facteurs activé fait de vous une cible beaucoup moins convaincante.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230910
"C'est ensemble qu'on avance"