Les protocoles d'authentification

[sommaire]

1. ## Objectifs

- Connaitre les protocoles d’authentification

- ## Présentation

  - L’authentification est une procédure permettant pour un système informatique de vérifier l’identité d’une personne ou d’un ordinateur et d’autoriser l’accès de cette entité à des ressources (systèmes, réseaux, applications).
  - L’identification permet de connaître l’identité d’une entité, alors que l’authentification permet de vérifier l’identité.
  - Il existe plusieurs facteurs d’authentification : utiliser une information que seul le prétendant connaît (mot de passe), possède (carte à puce), est (données biométriques), peut produire (un geste).
  - Les protocoles d’authentification décrivent les interactions entre un éprouveur et un vérifieur et les messages permettant de prouver l’identité d’une entité.
  - On distingue deux familles de protocoles d’authentification : l’**authentification simple** (un seul facteur d’authentification en jeu) et l’**authentification forte** (deux facteurs ou plus).
  - Par ailleurs, on parle d’authentification unique lorsqu’un utilisateur n’a besoin de procéder qu’à une seule authentification pour accéder à plusieurs applications informatiques.

- ## Facteurs d’authentification

  - Il existe 5 facteurs d'authentifications qui peuvent être utilisés dans le processus d’autorisation d’accès à des ressources bloquées et sécurisées :
  - Un facteur d'authentification est une catégorie de données d'authentification qui sert à vérifier l'identité.

  - **Facteur mémoriel (ce que l'on sait)**

    - Ce que l'on sait , ce l'on connait, c'est une information que l’utilisateur a mémorisée et que lui seul connait (exemple : un mot de passe, un nom d'utilisateur)

apcpedagogie.com

- Il s’agit d’une information qui n’est (idéalement) connue que de la personne dont l’identité est vérifiée et de la personne ou du processus qui la vérifie.
- cette catégorie de données d'authentification se compose des informations que l'utilisateur connaît, par exemple un code confidentiel, un nom d'utilisateur, un mot de passe ou la réponse à une question secrète.
- Parmi les éléments couramment utilisés comme **facteurs mémoriels**, on compte notamment les mots de passe, les phrases de passe, les mots de passe, les codes d’accès ou les NIP (acronyme signifiant Numéro d’identification personnel).
- Beaucoup de gens ne se rendent peut-être pas compte que les "questions secrètes", que certains sites Web vous font configurer en plus de votre mot de passe, appartiennent aussi à cette catégorie.

- **Facteur matériel (ce que l'on a)**

  - Ce que l'on possède, ce que l'on a, c'est une information que seul l’utilisateur possède et enregistrée dans un support (exemple : une clé USB).
  - Une carte de crédit ou de débit dans votre portefeuille ne sert pas uniquement à démontrer que vous avez été jugé apte à rembourser vos dettes; elle permet également de confirmer que votre institution financière a vérifié votre identité.
  - Mais les cartes d’identité et les cartes de paiement ne constitue pas la seule forme des facteurs matériels ou de possession. Tout ce qui peut être lié uniquement à vous peut être utile. Pensons par exemple à une adresse électronique, un appareil mobile ou un numéro de téléphone.
  - Des codes clés temporaires peuvent être générés par des sites en ligne et vous être envoyés par SMS, par appel vocal ou par courriel, pour vous permettre d’inscrire vos identifiants de connexion.

- **Facteur corporel (ce que l'on est)**

  - Ce que l'on est , c'est une information qui caractérise l’utilisateur avec une empreinte qui lui est propre (exemple : voix, pupille, empreinte digitale)
  - Les scanners d’empreintes digitales, l’exemple le plus courant, sont destinés à vérifier le motif unique sur le bout de vos doigts.
  - Certains téléphones intelligents sont maintenant équipés de scanners d'iris, qui recherchent les taches et les colorations uniques de vos yeux.
  - La US Customs and Border Patrol teste actuellement des scanners de reconnaissance faciale afin d’automatiser la vérification des pièces d’identité avec photo.

apcpedagogie.com

- **Facteur réactionnel**
    - Ce que l’on sait faire, c'est une information ou un geste que seul l’utilisateur peut produire (exemple : une signature)
- **Facteur de localisation**
    - Ce que l’on sait faire, c'est une information ou un geste que seul l’utilisateur peut produire (exemple : une signature)
    - Le "facteur de localisation" se base sur le fait qu'on on peut raisonnablement s'attendre à ce que vous vous trouviez en général à certains endroits (c'est-à-dire à la maison ou au travail) ou que vous utilisiez certaines machines spécifiques.
    - Évidemment, ce ne sera pas toujours le cas; cette information n’est donc pas très utile prise isolément. Si vous vous trouvez dans une région connue ou que vous utilisez une adresse IP ou MAC connue, vous pouvez l’utiliser comme deuxième facteur d’authentification en plus de saisir un nom d’utilisateur et un mot de passe.
    - Mais si vous n’êtes pas à cet endroit connu ou sur cette machine connue, il vous sera demandé d’utiliser un autre facteur d’authentification tel qu’un code clé.

Authentification à deux facteurs

- La connexion avec deux facteurs d’authentification est appelée "authentification à deux facteurs" ou "vérification en deux étapes" (2FA ou TFA en abrégé).
- Si un processus de connexion a activé (Two-factor authentication en anglais, 2FA), même si les utilisateurs fournissent leurs identifiants (accidentellement ou intentionnellement), leurs comptes peuvent toujours être protégés si l’attaquant n'a pas également accès au second facteur.
- La double authentification (Two-factor authentication en anglais, 2FA) ou vérification en deux étapes est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.
- Généralement l'une se présente sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.
- Ces deux facteurs représentent une chose possédée et une chose sue. Par exemple, Une carte bancaire est un bon exemple d'authentification à double facteur : la carte elle-même constitue l'élément physique, tandis que le code secret (ou PIN) représente les données qui y sont associées.

apcpedagogie.com

- La combinaison de ces deux éléments rend plus difficile l'accès à un compte bancaire par une personne non autorisée, celle-ci devant posséder à la fois l'élément physique (la carte) et le code secret.
- Ce type d'authentification permet de réduire l'incidence de fraudes en ligne, telles que l'usurpation d'identité et l'hameçonnage, étant donné que le mot de passe de la victime ne suffit pas à accéder aux informations

Applications

1. **Enoncé**

> *La double authentification est devenue essentielle pour sécuriser correctement des comptes contenant des données personnelles et professionnelles, comme sur Google, Facebook, Apple, Microsoft, Amazon ou encore PayPal. Voici un guide pour activer cette option sur les services les plus populaires.*

- Vous êtes appelés de présenter l'authentification à double facteurs de Google et de FaceBook.

- **Solutions proposées**

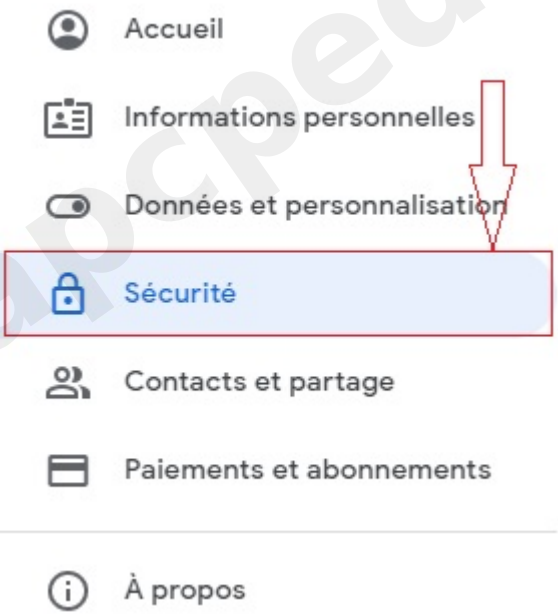
- **Google**

- L'authentification à double facteur avec Google peut se faire de plusieurs manières.
- La méthode d'activation diffère selon l'appareil utilisé (un ordinateur, un smartphone ou un IOS).
- **Configuration sur Smartphone**
  - Pour Android allez dans paramètres dans l'option Google puis dans compte Google puis dans sécurité activer la validation en deux étapes. Et vous suivez les instructions.
    - Pour les options de connexion à votre compte en cas de perte de téléphone, Google vous propose d'entrer un numéro secours ou encore il vous génère une série de code que vous pouvez utiliser pour vous connectes sur d'autres téléphone.
- **Configuration sur ordinateur**
- Vous vous connecter à votre compte Gmail rendez-vous dans l'onglet mon compte en haut à droite en cliquant sur la partie photo de profil.

apcpedagogie.com

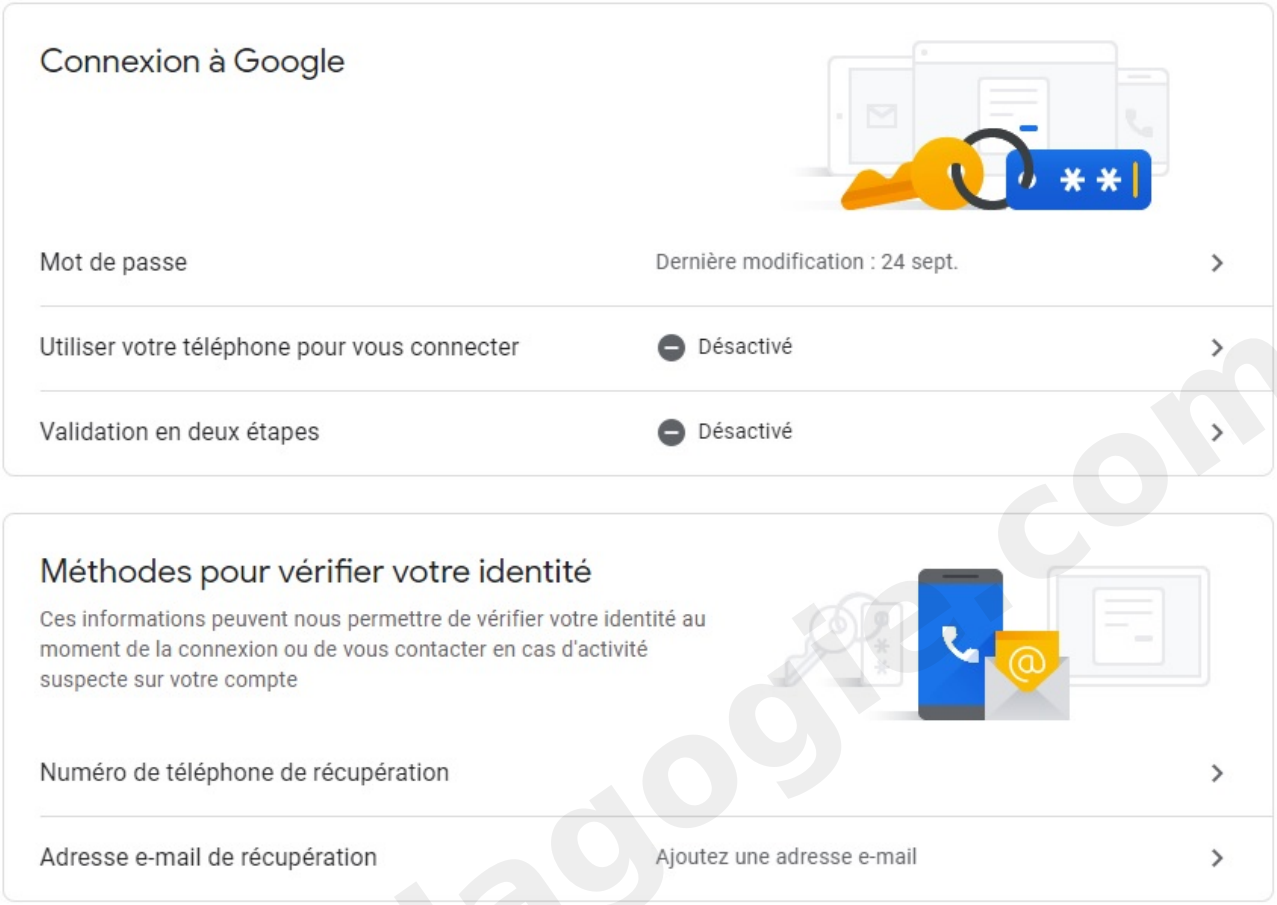


- Ensuite vous cliquer sur `Gérer votre compte Google`
- Ensuite vous allez dans la partie `sécurité` :



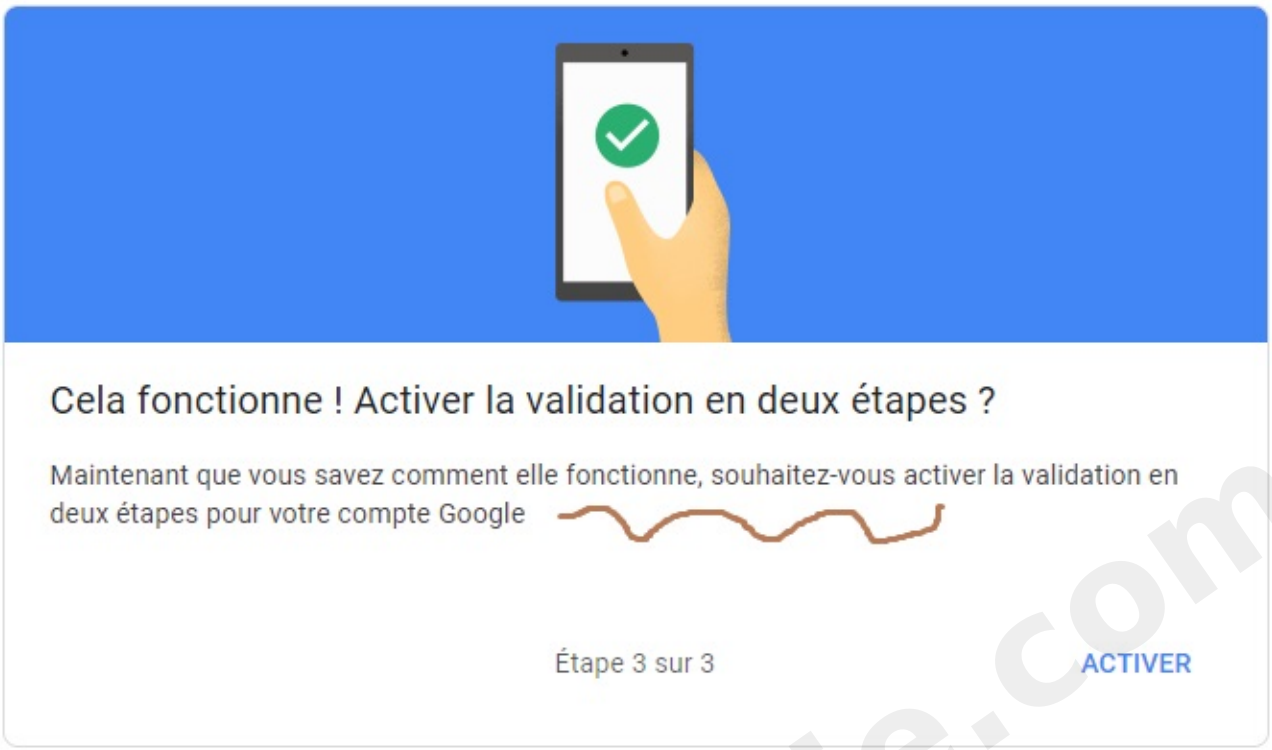
apcpedagogie.com

- Google vous demande d’entrer votre mot de passe ensuite un téléphone qui vous aidera à vous connecter.



- **Autrement**
  - Appelez la fonctionnalité s'appelle "Validation en deux étapes" et est proposée dans les options de sécurité sur la page de gestion de son compte. Rendez-vous sur **cette page** pour commencer la procédure.
  - Le géant va d’abord vous demander de configurer cette validation en deux étapes en vous envoyant un code à 6 chiffres par SMS ou par appel téléphonique grâce à votre numéro de téléphone mobile. Une fois cela fait, il est possible de configurer l'application **Google Authenticator** : elle génère le même type de code sans avoir besoin du réseau téléphonique.

apcpedagogie.com



- **FaceBOOK**
  - Facebook propose plusieurs façons d’activer l’authentification à deux facteurs.
  - Premièrement on peut recevoir des SMS sur son téléphone mobile en configurant l' **approbation de connexion**.
  - Les deux autres possibilités consistent à générer des codes sans avoir besoin d’une connexion au réseau mobile. Facebook conseille d’utiliser son application mobile qui intègre nativement le générateur de code.

apcpedagogie.com



Sources:

- *www.welivesecurity.com/fr/2019/05/31/authentification-101/*
- *www.lemagit.fr/definition/Authentification*
- *www.syloe.com/glossaire/authentification/*
- *www.syloe.com/glossaire/authentification/*

Cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/les-protocoles-dauthentification · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com