Identification et authentification

Par Patrick Sentinel – 29a.ca

Identification et authentification : comprendre ces concepts clés en sécurité informatique

Vous vous connectez à votre boîte mail, votre compte bancaire ou encore votre application de livraison préférée (parce que qui a le temps de cuisiner ?). Mais avez-vous déjà réfléchi à ce qui se passe en coulisses ? C'est là que **l'identification** et **l'authentification** entrent en jeu. Ces deux notions sont essentielles en cybersécurité, mais elles sont souvent confondues. Alors, accrochez-vous, on vous explique tout ça avec simplicité (et un peu d'humour) !

Identification vs authentification : Quelle différence ?

- **L'identification**, c'est dire **qui** vous êtes.
- **L'authentification**, c'est **prouver** que vous êtes bien cette personne.

Exemple simple :

Imaginez que vous arrivez à l'entrée d'une discothèque (même s'il n'y en a plus) :

Vous dites au portier : **"Je suis Oncle George 😉"** → C'est **l'identification**.

Le portier demande votre carte d'identité pour s'assurer que vous ne mentez pas → C'est **l'authentification**.

En informatique, c'est pareil :

Quand vous entrez votre **nom d'utilisateur** ou votre **adresse électronique** pour vous connecter à un site, c'est **l'identification**.

Quand vous saisissez votre **mot de passe**, scannez votre empreinte digitale ou utilisez un code reçu par SMS, c'est **l'authentification**.

Comment fonctionne l'authentification ?

Pour vérifier votre identité, un système d'authentification utilise **trois types de preuves** :

Ce que vous savez (facteur de connaissance)

C'est la méthode classique :
✓ Un **mot de passe** (par exemple, "123456", mais promis, on y revient 👀);
✓ Un **code PIN**;
✓ Une **réponse à une question secrète** ("Le prénom de votre premier animal ?" Spoiler : les hackers devinent souvent).

📌 **Problème** : Si quelqu'un devine ou vole votre mot de passe, il peut se connecter à votre place.

Ce que vous possédez (facteur de possession)

Ici, il faut un objet physique :
✓ Un téléphone qui reçoit un code par SMS ou *Authenticator*;
✓ Une clé de sécurité USB;
✓ Une carte à puce.

📌 Problème : Si vous perdez votre téléphone ou votre clé USB... Ça devient compliqué !

Ce que vous êtes (facteur biométrique)

✓ Empreinte digitale.
✓ Reconnaissance faciale.
✓ Analyse de la rétine ou de l'iris (un peu futuriste, mais ça existe !).

La biométrie est une méthode d'authentification de plus en plus courante, notamment sur les smartphones. Vous utilisez sûrement Face ID ou votre empreinte digitale pour déverrouiller votre téléphone.

👉 Mais peut-on utiliser la biométrie seule pour s'authentifier ?
Oui, c'est possible ! Par exemple, votre téléphone peut être configuré pour ne s'ouvrir qu'avec votre empreinte digitale, sans besoin de mot de passe. Certains bâtiments sécurisés fonctionnent aussi avec des scanners rétiniens sans autre vérification.

📌 Mais attention ! La biométrie seule n'est pas infaillible.

Certains systèmes de reconnaissance faciale ont été trompés par de simples photos. Des hackers ont réussi à reproduire des empreintes digitales en 3D pour contourner des verrous biométriques. Contrairement à un mot de passe, vous ne pouvez pas "changer" vos empreintes digitales ou votre visage si elles sont compromises. 😅

C’est pourquoi, dans la plupart des systèmes critiques, la biométrie est souvent couplée avec un autre facteur d’authentification, comme un code PIN ou un mot de passe.

L’authentification à plusieurs facteurs (MFA) : La vraie sécurité

Comme une seule méthode peut être insuffisante, les experts recommandent l’**authentification à plusieurs facteurs** (**MFA** pour *Multi-Factor Authentication*).

Comment ça marche ?

Vous combinez **deux** ou **trois** preuves pour sécuriser votre connexion. Exemple :

- Vous entrez votre **mot de passe** (*ce que vous savez*);
- Vous recevez un **code sur votre téléphone** (*ce que vous possédez*).

Même si un hacker vole votre mot de passe, il lui faudra aussi votre téléphone… et à moins qu’il ne l’ait aussi (et là, on a un vrai problème), il sera bloqué.

📌 **Bon à savoir** : Certaines entreprises imposent la MFA, notamment pour les comptes sensibles (banques, messageries professionnelles, réseaux sociaux).

Les erreurs classiques à éviter

💀 **1. Utiliser le même mot de passe partout**
Un hacker récupère un seul de vos mots de passe et BAM ! Il accède à tous vos comptes.

💀 **2. Choisir un mot de passe trop simple**
Si votre mot de passe est "123456", "password" ou "qwerty", félicitations, vous venez de faciliter la tâche des pirates.

💀 **3. Ne pas activer la double authentification**
Si un service propose la MFA et que vous ne l’activez pas, c’est comme laisser la porte de chez vous ouverte en vacances.

💀 **4. Noter ses mots de passe sur un post-it**
Oui, même si c’est caché sous le clavier, ce n’est pas une bonne idée.

Comment bien gérer ses identifiants et mots de passe ?

✓ Utiliser un gestionnaire de mots de passe (comme *Bitwarden*, *1Password* ou *LastPass*);
✓ Activer l'authentification à deux facteurs dès que possible;
✓ Ne jamais utiliser le même mot de passe sur plusieurs sites;
✓ Changer ses mots de passe après une fuite de données.

Identification, authentification… et après ?

Une fois que vous êtes authentifié, il y a une dernière étape : **l'autorisation**.

- **Identification** : "Qui êtes-vous ?"
- **Authentification** : "Prouvez-le !"
- **Autorisation** : "Ok, maintenant, qu'avez-vous le droit de faire ?"

Par exemple, même si vous êtes connecté à votre entreprise, cela ne signifie pas que vous avez accès aux fichiers secrets du patron (désolé 😆).

Conclusion : Soyez le gardien de votre propre sécurité

Se faire pirater, ça n'arrive pas qu'aux autres. En adoptant de bonnes pratiques d'identification et d'authentification, vous réduisez considérablement les risques.

Alors, prenez quelques minutes pour :
✅ Activer la double authentification.
✅ Mettre à jour vos mots de passe.
✅ Tester un gestionnaire de mots de passe.

Et surtout… **arrêtez d'utiliser "123456"**. Merci. 😊