UNIVERSITÉ DE TOULON

Le renforcement de la sécurité des comptes numériques

www.univ-tln.fr

La sécurité des comptes numérique fragile

L'usage quotidien des outils numériques dans l'environnement professionnel ou d'études nécessite pour chaque utilisateur la création d'un compte numérique. Celui-ci repose sur la création d'un login et d'un mot de passe. Ce système est aujourd'hui quotidiennement victime d'attaques sous diverses formes qui visent à développer la cybercriminalité et l'usage frauduleux des données personnelles.

Le renforcement de la sécurité des comptes numériques

Pour renforcer la sécurité des comptes et limiter l'usurpation numérique, de nombreux services en ligne comme les banques ou les sites de e-commerce ont mis en place un système d'authentification forte multifacteur (MFA). Cette méthode d'authentification dépasse le simple mot de passe en exigeant la vérification de plusieurs éléments pour garantir l'identité de l'utilisateur.
Les avantages sont nombreux et contribuent à renforcer la sécurité des informations sensibles.

1 Renforcement de la sécurité

En exigeant plusieurs formes d'identification, tels que des codes PIN, des empreintes digitales, elle complique considérablement la tâche des pirates informatiques qui tentent d'accéder illégalement à un compte.

2 Réduction des risques

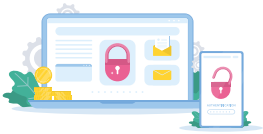
Les mots de passe faibles et la compromission de compte sont souvent la principale porte d'entrée pour les attaquants. Avec le MFA, même si un mot de passe est compromis, l'accès au compte reste limité sans la validation des autres facteurs d'authentification.

3 Protection contre le phishing

Les attaques de phishing visent à tromper les utilisateurs pour obtenir leurs identifiants. Le MFA ajoute une couche de protection en demandant des informations supplémentaires que les attaquants ne peuvent pas facilement dérober par le biais d'e-mails frauduleux.

4 Conformité réglementaire

De nombreuses réglementations en matière de protection des données exigent désormais l'utilisation de l'authentification forte multifacteur pour garantir la sécurité des informations personnelles.



L'Université de Toulon déploie l'authentification forte multifacteur

À l'Université de Toulon, l'authentification forte multifacteur (MFA) sera mise en œuvre pour renforcer la sécurité des services numériques et protéger l'accès aux comptes des utilisateurs.

Voici les étapes du processus :

1

Activation (Enrôlement) du MFA

Vous devrez installer et paramétrer une première fois l'application associée à l'authentification forte multifacteur : Authenticator. Vous devrez choisir un code PIN personnel qui servira à sécuriser vos accès.

2

Identifiant et Mot de passe

Lors de votre connexion aux services numériques de l'Université comme la messagerie Partage, vous utiliserez votre identifiant et votre mot de passe habituels pour accéder à votre compte.

3

Ouverture d'Authenticator

Après avoir renseigné votre login et mot de passe, un message vous invitera à ouvrir Authenticator sur votre ordinateur et/ou votre smartphone pour vous demander votre code PIN.

4

Code PIN pour sécuriser la liaison

Le code PIN que vous avez choisi lors de l'activation sera nécessaire pour sécuriser votre connexion. Cela ajoute une couche supplémentaire de sécurité, garantissant que même si quelqu'un obtient votre identifiant et mot de passe, il ne pourra pas accéder à votre compte sans le code PIN associé et l'application que vous aurez activée.

5

Sécurité renforcée

Grâce à ce processus, l'Université de Toulon renforce considérablement la sécurité de l'accès aux comptes des utilisateurs et de son système d'information. Même en cas de compromission potentielle de vos informations d'identification de base, la nécessité de prouver votre identité via l'application Authenticator et le code PIN offre une protection supplémentaire.

L'adoption de l'authentification forte multifacteur à l'Université de Toulon s'inscrit dans une démarche proactive visant à prévenir les risques liés à la sécurité informatique, assurant ainsi la confidentialité des données et la protection des comptes des utilisateurs. Ce processus contribue à créer un environnement numérique plus sécurisé et fiable pour la communauté universitaire. Plus d'informations sur le projet : https://dsiun.univ-tln.fr

UNIVERSITÉ DE TOULON

DÉPASSONS L'HORIZON

Direction du Système d'Information et des Usages Numériques
Université de Toulon
CS 60 584 • 83041 Toulon CEDEX 9
www.univ-tln.fr