Guide d'utilisation Protection des ressources Microsoft 365

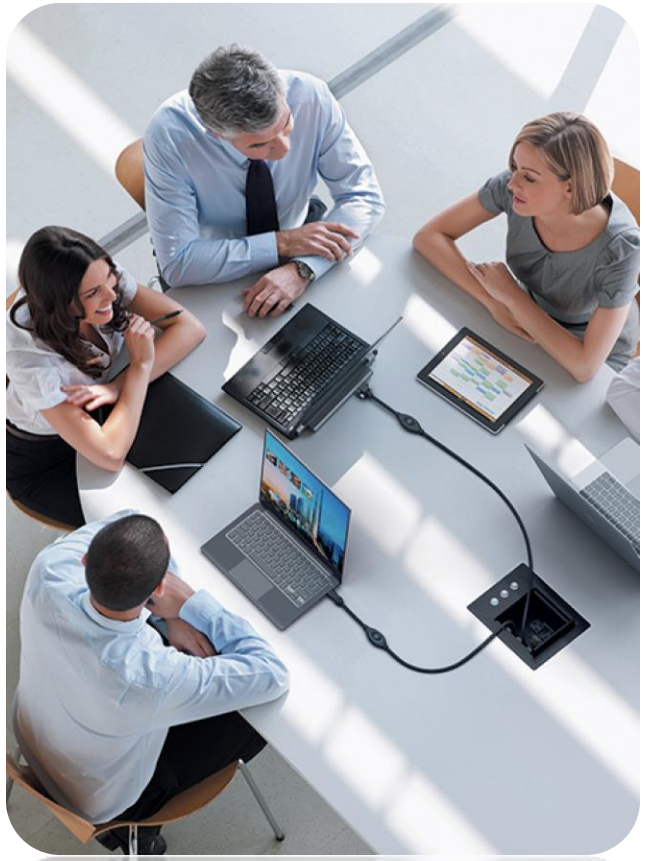
Présentation synthétique de votre assistant personnel CARE

GROUPE PASTEUR MUTUALITÉ

Guide d’utilisation – Protection Microsoft 365

Présentation de l’assistant personnel CARE

- **Objectif :**
  - Faciliter la compréhension des enjeux liés à l’utilisation des ressources Microsoft 365 en identifiant les anomalies à l’aide d’un tableau de bord



- **Principes fondamentaux :**
  - Présentation de l’assistant personnel de sécurité
  - Identification des ressources protégées
  - Présentation du tableau de bord : Profil de sécurité
  - Mise en place de notifications utilisateurs
  - Campagne périodique de validation du profil de sécurité

FLASH CYBERSECURITE

ACTIVATION DE LA PROTECTION DE L'ENVIRONNEMENT MICROSOFT 365

Dans le cadre de la mise en œuvre du projet de sécurisation de l'accès aux données d'entreprise, vous allez bénéficier d'une protection globale de vos accès à Microsoft 365. Ainsi, en cas d'activité suspecte sur votre environnement, des investigations seront menées pour s'assurer de la légitimité de ces accès.

Cette mise sous protection, va vous permettre d'être acteur de la sécurité à apporter sur vos accès et d'être averti en temps réel, lors d'une situation pouvant être à risque :

- accès à votre compte par un nouvel utilisateur,
- connexion à votre compte depuis une nouvelle localisation,
- synchronisation d'un nouvel appareil mobile,
- transfert automatique de courriels vers une boîte externe.

Phase#1 : observation, non intrusive, initiée en vue d'établir votre profil de sécurité.

Phase#2 : validation du profil d'utilisation de votre environnement Microsoft 365, vous offrant une réelle visibilité sur vos accès, puis en quelques clics, de signaler au RSSI, tout écart avec vos usages habituels.

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

www.gpm.fr

Présentation de l'assistant personnel CARE

Protection Microsoft 365

Présentation de l'assistant personnel CARE et identification des ressources protégées

- **Présentation de l'Assistant personnel CARE**
  - Mise à disposition d'un assistant personnel de sécurité, nommé **CARE pour protéger les outils collaboratifs Microsoft 365** contre un accès illégitime ou d'une divulgation de vos données

- **Ressources protégées par votre assistant CARE**
  - Boîte mail et calendrier Outlook
  - Espace de stockage personnel OneDrive
  - Bibliothèques Teams et SharePoint

Assistant personnel CARE : Profil de sécurité et notifications

Protection Microsoft 365

Composition de l'assistant personnel CARE : 2 caractéristiques fondamentales

- **Profil de sécurité**
  - Tableau de bord personnel vous permettant de suivre et de maîtriser la sécurité de vos ressources Microsoft 365 en corrigeant toutes anomalies que vous constaterez

- **Notifications aux utilisateurs**
  - Notifications vous permettant de valider ou de signaler directement aux équipes de sécurité en cas de comportement anormal sur vos ressources protégées Microsoft 365 *(accès malveillants ou inhabituels)*
  - Notifications immédiates auprès de l'utilisateur et investigations menées en cas d'activité suspecte

Assistant personnel CARE

L'utilisateur GPM est un acteur engagé dans la sécurité à apporter sur ses propres ressources

Présentation du profil de sécurité

Qu'est-ce que le profil de sécurité ?

- Tableau de bord personnel simple et interactif vous permettant de suivre et de maîtriser la sécurité de vos ressources Microsoft 365
- Réalisation de contrôles efficaces sur vos ressources Microsoft 365

Qu'est-ce qu'il vous permet de contrôler ?

- **Configuration générale**
  - Identification des pays habituels de connexion et de vos appareils synchronisés sur votre compte *(ex : 2 appareils synchronisés sur votre compte « Ipad et Iphone »)*
- **Boîte mail et calendrier**
  - Identification des autorisations et des règles de configuration *(ex : transfert automatique)*
- **Espace de stockage personnel OneDrive**
  - Identification des partages *(ex : partage d'un document confidentiel à des externes)*
- **Bibliothèques Teams et SharePoint**
  - Identification des autorisations *(ex : collaborateurs ayant accès à une équipe Teams)*

Assistant personnel CARE

En cas de comportement anormal, émission immédiate d'une alerte

Notifications utilisateurs

Quel est le but d'une notification ?

- Permettre à un utilisateur de valider un accès inhabituel ou de signaler directement aux équipes de sécurité un comportement anormal sur sa ressource
- Notifications immédiates par e-mail permettant à l'utilisateur d'alerter les équipes de sécurité pour réagir efficacement en menant des investigations en cas d'activité suspecte

Quels sont les cas d'utilisation ?

Ma boîte mail et mon calendrier sont accessibles à des collaborateurs de l'entreprise.
Est-ce légitime ?

Un nouveau partage externe via OneDrive contenant des données sensibles, est réalisé.
Est-ce légitime ?

Je me connecte habituellement depuis la France, et il est constaté une connexion depuis la Suède.
Est-ce légitime ?

Campagne périodique de validation

GROUPE PASTEUR MUTUALITÉ

PROTECTION DE MICROSOFT 365 par CARE

Powered by IDECSI

La mise sous protection, va vous permettre d'être acteur de la sécurité à apporter sur vos accès et d'être averti en temps réel, lors d'une situation pouvant être à risque. Le programme CARE met à disposition des collaborateurs du Groupe des solutions adaptées pour protéger les données d'entreprise.

Visualisation des droits appliqués sur boîte mail ou sur votre calendrier

Informations sur les modalités de connexion (*appareil mobile, mode d'accès ou localisation*)

Informations en temps réel sur un transfert automatique de mail vers une boîte externe

Visualisation de mes partages OneDrive ou des membres d'une Equipe Teams

Une validation de votre profil de sécurité en 4 étapes

1. Vérification des informations de connexion

Les connexions indiquées sur mon profil sont-elles légitimes ?

- origine des connexions
- appareils mobiles

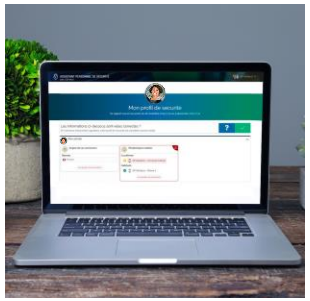
Sinon, cliquer sur Corriger pour signaler une anomalie.

2. Vérification des permissions sur votre mail et calendrier

Quels sont les permissions appliquées sur votre boîte mail et votre calendrier ?

Ces permissions sont-elles légitimes ?

Sinon, cliquer sur Corriger pour signaler une anomalie.



3. Vérification des permissions sur votre OneDrive

Quels sont les partages que vous avez réalisés avec OneDrive ?

Ces partages sont-ils d'actualité ? Doivent-ils être supprimés ?

Sinon, cliquer sur Corriger pour signaler une anomalie.

4. Vérification des permissions sur vos bibliothèques Teams et SharePoint

Quels sont les propriétaires et les membres de ces bibliothèques ?

Des documents sont-ils accessibles depuis l'extérieur ?

Sinon, cliquer sur Corriger pour signaler une anomalie.

Activer la mise sous protection en temps réel, faisant suite à vos vérifications, en validant votre profil d'utilisation.

LA SÉCURITÉ EST L'AFFAIRE DE TOUS, ET MAÎTRISONS LA CONFIDENTIALITÉ DE NOS DONNÉES D'ENTREPRISE.

FLASH CYBERSECURITE

MISE EN PLACE DE VOTRE PROTECTION PERSONNALISÉE

La phase d'observation a permis d'établir un profil d'utilisation qui vous permettra de visualiser l'intégralité de votre activité dédiée à Microsoft 365.

Comme indiqué, ce profil va vous offrir de la visibilité sur vos accès et vous permettre de constater le cas échéant des éventuelles déviances :

- accès à votre compte par un nouvel utilisateur,
- connexion à votre compte depuis une nouvelle localisation,
- synchronisation d'un nouvel appareil mobile,
- transfert automatique de courriels vers une boîte externe.

Vous aurez également la possibilité de vous assurer de la confidentialité appliquée à votre environnement, en vérifiant à tout moment qui accède à vos fichiers ou à votre boîte mail.

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

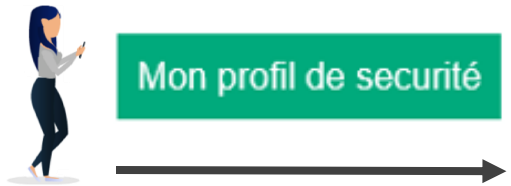
www.gpm.fr

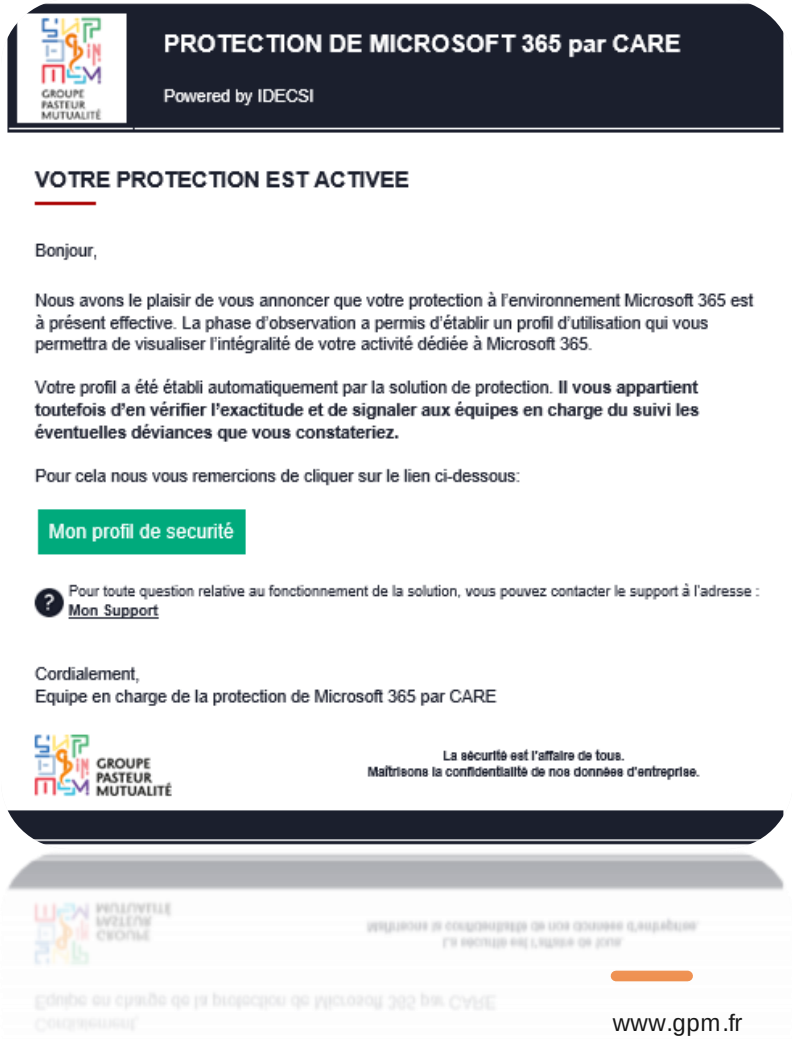
Protection Microsoft 365

Campagne périodique de validation de votre profil de sécurité

- **Mise en place d'une protection personnalisée**
  - Apprentissage par votre assistant personnel grâce à une phase d'observation pour construire votre profil de sécurité
  - Validation du profil de sécurité, par le collaborateur pour s'assurer de la légitimité des droits
  - Campagne périodique de validation du profil de sécurité, pour recertifier vos droits et accès

- À la fin de la période d'observation, vous recevrez un e-mail (no-reply@idecsi.fr) vous informant que votre protection a été activée et prête pour validation





PROTECTION DE MICROSOFT 365 par CARE

Powered by IDECSI

VOTRE PROTECTION EST ACTIVEE

Bonjour,

Nous avons le plaisir de vous annoncer que votre protection à l'environnement Microsoft 365 est à présent effective. La phase d'observation a permis d'établir un profil d'utilisation qui vous permettra de visualiser l'intégralité de votre activité dédiée à Microsoft 365.

Votre profil a été établi automatiquement par la solution de protection. **Il vous appartient toutefois d'en vérifier l'exactitude et de signaler aux équipes en charge du suivi les éventuelles déviances que vous constateriez.**

Pour cela nous vous remercions de cliquer sur le lien ci-dessous:

Mon profil de securité

Pour toute question relative au fonctionnement de la solution, vous pouvez contacter le support à l'adresse : Mon Support

Cordialement,
Equipe en charge de la protection de Microsoft 365 par CARE

GROUPE PASTEUR MUTUALITÉ

La sécurité est l'affaire de tous.
Maîtrisons la confidentialité de nos données d'entreprise.

GROUPE
PASTEUR
MUTUALITÉ

POUR NOUS, PROFESSIONNELS DE SANTÉ

www.gpm.fr