Guide d’utilisation Protection Microsoft 365

Foire aux questions

GROUPE PASTEUR MUTUALITÉ

Foire aux questions

FLASH CYBERSECURITE

FOIRE AUX QUESTIONS

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité. La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données. Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Outlook : Application offrant les fonctionnalités courrier et calendrier, qui permettent d'envoyer, de recevoir et gérer des courriels. Le calendrier intégré d'Outlook permet quant à lui, de suivre les rendez-vous (*professionnels ou personnels*) et les événements.

Exemples de situations à risque : accès à votre compte Microsoft 365 par un nouvel utilisateur, faisant suite à configuration illégitime sur votre boîte (**opération d'administration, modification de permissions ou vol d'identifiants**). Ceci afin d'accéder à vos courriels ou de réaliser une campagne d'hameçonnage en interne ou à l'extérieur de l'organisation.

OneDrive : Application permettant aux collaborateurs d'accéder à des fichiers, de les partager et de collaborer :

- accès aux travaux en toute simplicité à partir de tous les appareils,
- partage rapide et collaboration intelligente à l'intérieur ou à l'extérieur de votre organisation,
- facilitation du stockage de fichiers et d'accès

Exemples de situations à risque : modification involontaire de la configuration d'un partage ou **accès à un partage anonyme** permettant à un tiers non autorisé d'accéder aux données .

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

www.gpm.fr

FLASH CYBERSECURITE

FOIRE AUX QUESTIONS

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité. La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données. Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Mode d'accès : Microsoft 365 est un espace collaboratif, accessible selon des modalités d'accès :

- accès en ligne
- accès depuis un poste de travail
- accès appareil mobile

Exemples de situations à risque : synchronisation d'un nouvel appareil mobile par un tiers ou un **accès en ligne inhabituel** permettant ainsi à un cybercriminel ou à un utilisateur malintentionné d'accéder à l'ensemble des données .

Origine des localisations : Identification des localisations (*principalement la France pour les utilisateurs de GPM*) lors d'une connexion aux outils Microsoft 365.

Exemples de situations à risque : connexion à votre compte depuis une nouvelle localisation (*Nigéria, pays d'Asie ou Russie,* …) ou **connexion simultanée** depuis diverses localisations (*France et Egypte*). Ces actions sont généralement réalisées par un cybercriminel mais peuvent être légitimes lors d'un déplacement d'un collaborateur (*exemple lors de la période estivale*).

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

www.gpm.fr

FLASH CYBERSECURITE

FOIRE AUX QUESTIONS

L'accès aux applications Outlook, Teams, OneDrive, … est fondamental pour un collaborateur pour exercer son activité. La compromission de vos identifiants est un risque réel et il en devient critique de maîtriser l'accès à vos données. Cette foire aux questions a pour but de répondre à vos interrogations sur des éventuelles situations à risque.

Transfert automatique : Fonctionnalité permettant de transférer ou de rediriger vos messages électroniques vers une autre boîte mail (*interne ou externe à l'organisation*).

Exemple de situation à risque : transfert automatique par un cybercriminel de courriels vers une boîte externe lors d'une campagne d'hameçonnage pour effacer les traces des messages envoyés.

Faisant suite à la constatation d'une déviance par un utilisateur, quels sont les étapes que je vais devoir suivre ?
Pour rappel, une déviance peut être un accès non autorisé à votre compte, une synchronisation d'un nouvel appareil mobile ou toute autre action effectuée sur votre environnement qui ne serait pas à votre initiative.

1. **Cliquer sur le bouton Corriger :** ceci permettra de signaler la déviance
2. **Remédier :** l'équipe technique analysera la situation puis procédera à la remédiation si nécessaire pour remédier
3. **Valider le profil :** à l'issue de la remédiation globale, il sera demandé de valider votre profil afin que vous puissiez être alerté en temps réel

PROGRAMME DE
CYBERSÉCURITÉ CARE

TOT'M

PLUS DE DÉTAIL SUR TOT'M

#Cybersécurité #CARE #Protéger #Zero Trust

Office 365

www.gpm.fr

GROUPE
PASTEUR
MUTUALITÉ

**POUR NOUS,
PROFESSIONNELS
DE SANTÉ**

www.gpm.fr