MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

Février 2024

LA THEMATIQUE DU MOIS :
LA DOUBLE AUTHENTIFICATION (2FA)

Qu'est ce que la double authentification ?

La double authentification, aussi appelée validation ou vérification en deux étapes, ou encore « 2FA » est un renforcement de la sécurité des comptes. Elle permet d'éviter un éventuel piratage en agissant comme une protection supplémentaire en cas de vol du mot de passe.

COMMENT CA FONCTIONNE ?

La double authentification peut s'activer sur de nombreux services en ligne, la messagerie, les réseaux sociaux ainsi que les sites internet de ventes en ligne.
Une fois activée**, en plus de votre nom de compte et de votre mot de passe**, ce service vous demandera une confirmation en fournissant un code provisoire reçu par SMS ou par mail. Cette authentification peut également d'effectuer par une application, une clé spécifique ou par reconnaissance biométrique. En fonction du service, cette **demande de confirmation** pourra vous être demandée à la première connexion ou à chaque connexion, à intervalle régulier, mais surtout à chaque fois qu'un nouvel équipement inconnu par le service concerné tentera de se connecter à votre compte.
Vous seul pourrez donc autoriser un nouvel appareil à se connecter à vos comptes protégés par la double authentification.

A QUOI CA SERT ?

À bloquer toute tentative d'accès à votre compte, à votre insu avec votre mot de passe.

Dans ce cas, si une personne malveillante essayait d'accéder à votre compte avec votre mot de passe, elle en serait empêchée et vous recevriez une alerte vous notifiant que quelqu'un a essayé de s'y connecter.

Il faudra alors changer de mot de passe immédiatement pour bloquer une éventuelle tentative de connexion et de piratage de votre compte.

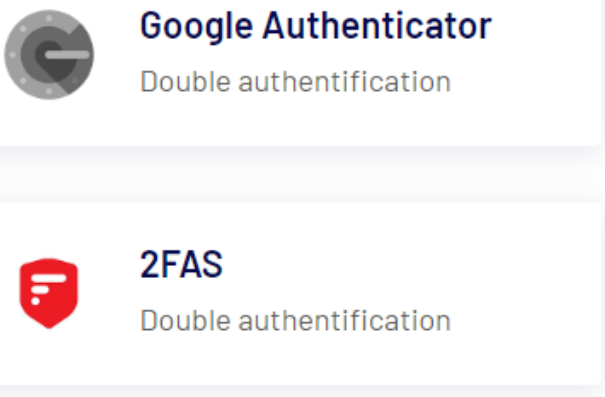
LES METHODES DE DOUBLE AUTHENTIFICATION

Par SMS : Elle est probablement la plus courante. Le service vous transmettra un SMS contenant un code à usage unique à chaque connexion sur votre compte. Cette méthode n'est pas la plus sécurisée mais elle est la plus simple à mettre en œuvre.

Par notification : La notification permet de valider une connexion depuis un nouvel appareil. Une notification est envoyée sur votre smartphone qu'il suffira de valider.

Par application : Cette méthode est plébiscitée pour son haut niveau de sécurité. Une fois l'application installée sur votre smartphone, il faut scanner le QR code qui apparait dans l'application. L'application génère alors un code à 6 chiffres à usage unique et différent toutes les 30 secondes.

EXEMPLES D'APPLICATION 2FAS ?



POUR CONCLURE:

La double authentification est une mesure pratique et peu contraignante qui **augmente considérablement la sécurité de vos comptes**. Cybermalveillance.gouv.fr vous conseille donc fortement d'activer la double authentification sur vos comptes chaque fois que vous le pouvez. Voici quelques exemples de services proposant la double authentification :

- Amazon
- Apple iCloud
- Discord
- Dropbox
- eBay
- Facebook
- Gmail
- Google Drive
- Impôts.gouv.fr
- Instagram
- La Poste
- Le Bon Coin
- LinkedIn
- OneDrive
- Outlook/Hotmail
- PayPal
- Skype
- Snapshat
- Teams
- Telegram
- TikTok
- Twitch.tv
- X (Twitter)
- Vinted
- WhatsApp
- Yahoo Mail
- Youtube
- Zoom

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de Gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L.GRAU
Rédacteurs: ADJ M.KNOBLOCH – ADJ E.DUBOIS
MAJ (ER) WOLFERT

Si vous souhaitez recevoir cette lettre, envoyez un mail à:
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: