



3 ASTUCES PEU CONNUES POUR ÉVITER TOUT PIRATAGE SUR TON PC



01

**UTILISEZ DES MOTS
DE PASSE FORTS ET
LES PROTEGER**



02



**ACTIVEZ LA
DOUBLE
AUTHENTIFICATION**

03

**NE BRANCHEZ
JAMAIS DE CLES
USB INCONNUES**



01

UTILISEZ DES MOTS DE PASSES FORTS ET LES PROTÉGER



LES MOTS DE PASSE SONT LE PREMIER OBSTACLE À FRANCHIR DES PIRATES INFORMATIQUES. IL EST IMPORTANT D'UTILISER DES MOTS DE PASSE FORTS ET DE LES PROTÉGER AFIN DE MAXIMISER TA PROTECTION.

AYEZ-UN MOT DE PASSE AVEC 8
CARACTÈRES MINIMUM EN MÉLANGEANT
ABSOLUMENT DES CHIFFRES, DES
LETTRES ET DES CARACTÈRES SPÉCIAUX !

EXEMPLE ✓

DES LETTRES "CKT987++" DES CHIFFRES DES CARACTÈRES SPÉCIAUX

MOT DE PASSE À BANNIR ✗

QUE DES CHIFFRES "987" QUE DES LETTRES "VÉLO"

IMPORTANT : ⚠

N'UTILISEZ PAS LE MÊME MOT DE PASSE
POUR TOUS VOS COMPTES, CAR SI UN
PIRATE INFORMATIQUE PARVIENT À
VOLER CE MOT DE PASSE, IL AURA ACCÈS
À TOUTES VOS INFORMATIONS SENSIBLES.



SOLUTION : 💡

POUR ÉVITER CELA, VOUS DEVEZ UTILISER
UN MOT DE PASSE DIFFÉRENT POUR
CHAQUE COMPTE ET LES STOCKER DANS
UN GESTIONNAIRE DE MOTS DE PASSE
SÉCURISÉ.

CELUI LÀ PAR EXEMPLE...



02

ACTIVEZ LA DOUBLE AUTHENTIFICATION



LA DOUBLE AUTHENTIFICATION AJOUTE UNE COUCHE SUPPLÉMENTAIRE DE SÉCURITÉ À VOS COMPTES EN LIGNE EN EXIGEANT UNE DEUXIÈME FORME D'AUTHENTIFICATION (COMME UN CODE DE SÉCURITÉ ENVOYÉ À VOTRE TÉLÉPHONE) EN PLUS DE VOTRE MOT DE PASSE.

PAR EXEMPLE :



ET



OFFRENT LA DOUBLE
AUTHENTIFICATION. IL EST IMPORTANT
D'ACTIVER CETTE FONCTIONNALITÉ À
CHAQUE FOIS QU'ELLE EST
DISPONIBLE.

UN CODE DE SÉCURITÉ ENVOYÉ À VOTRE
TÉLÉPHONE) EN PLUS DE VOTRE MOT DE
PASSE.

The image shows two side-by-side screenshots. The left screenshot is from the Google Authenticator app, displaying a notification: "Vous y êtes invité, saisissez ce code de validation lorsque vous vous connectez à votre compte :". Below this, it shows the Google logo, the code "045495" in a red box, and the email address "@gmail.com". A red arrow points from the code to the right screenshot. The right screenshot is from the Google login page, titled "Validation en deux étapes". It shows a smartphone icon and the text "Saisissez le code de validation généré par votre application pour appareil mobile." Below this is a text input field labeled "Saisissez le code" in a red box, a blue "Valider" button, and a checkbox for "Mémoriser cet ordinateur pendant 30 jours". At the bottom, there is a link: "Vous rencontrez des problèmes avec votre code ?".

03

NE BRANCHEZ JAMAIS DE CLES USB INCONNUES



SI C'EST UNE CLÉ USB QUI NE VOUS APPARTIENT PAS, VOUS VOUS EXPOSEZ À UN DANGER POUR VOTRE PC. CELA AUGMENTE LES RISQUES DE PIRATAGE ET D'INFECTION PAR DES LOGICIELS MALVEILLANTS. LES CLÉS USB PEUVENT CONTENIR DES VIRUS ET DES PROGRAMMES MALVEILLANTS QUI PEUVENT COMPROMETTRE LA SÉCURITÉ DE VOTRE ORDINATEUR.

SI VOUS DEVEZ TRANSFÉRER DES DONNÉES, UTILISEZ PLUTÔT DES MÉTHODES PLUS SÛRES :



TELLES QUE LE PARTAGE DE FICHIERS VIA LE CLOUD



LA TRANSMISSION DE FICHIERS VIA DES SERVICES EN LIGNE DE TRANSFERT DE FICHIERS SÉCURISÉS

COMME GOOGLE DRIVE



COMME WE TRANSFER

SI VOUS DEVEZ ABSOLUMENT UTILISER UNE CLÉ USB, ASSUREZ-VOUS QU'ELLE EST DE SOURCE FIABLE ET SCANNÉE PAR UN LOGICIEL ANTIVIRUS AVANT DE L'UTILISER.

