- [Instructeur] Bonjour tout le monde !
Nous allons parler de BitLocker et de BitLocker To Go.
La présentation va porter sur le chiffrement de votre lecteur.
Qu'il s'agisse d'un lecteur de données fixe,
c'est-à-dire le disque dur à l'intérieur de votre tour ou de votre ordinateur portable,
ou d'un lecteur flash USB ou
de stockage amovible,
qui sera chiffré avec BitLocker To Go.
Dans les deux cas, nous voulons chiffrer nos
données pour les protéger.
C'est parti.
Je clique sur le bouton Démarrer de Windows,
puis sur Panneau de configuration.
Nous y voilà !
Dans Windows 10, Windows 8 et Windows 7,
vous allez pouvoir utiliser BitLocker.
Windows 7 Enterprise et Ultimate l'utilisent aussi,
ainsi que Windows 8 Pro et Enterprise.
Si comme moi vous utilisez Windows 10,
Windows 10 Pro, Enterprise et Education,
ils prennent tous en charge BitLocker.
Je clique
sur Chiffrement de lecteur BitLocker
dans le Panneau de configuration, et dans la fenêtre qui s'ouvre,
je vois le lecteur du système d'exploitation,
qui est le lecteur de données fixe,
c'est-à-dire le disque C.
Il y a aussi un disque de données amovible,
le lecteur flash nommé IMPORTANT, c'est-à-dire le lecteur E.
Nous allons commencer par le disque amovible,
car il contient les fichiers que vous
emportez avec vous lors de vos déplacements, et il est très facile à perdre.
Si vous avez des données sensibles sur un disque amovible,
il est conseillé de les chiffrer
pour empêcher d'autres personnes d'y accéder
à moins qu'elles utilisent le mot de passe de déchiffrement.
Je vais donc cliquer sur Activer BitLocker
sur le lecteur flash connecté à ma machine.
BitLocker démarre, il initialise le lecteur flash
et demande comment je souhaite déverrouiller ce lecteur.
Il s'agit de la méthode
qui sera utilisée pour déchiffrer le contenu de mon lecteur flash.
Je peux utiliser un mot de passe ou une carte à puce,
ou une combinaison des deux.

La carte à puce doit
être insérée dans votre machine,
et lorsqu'elle est insérée,
je vais pouvoir déchiffrer
le contenu du lecteur flash.
Étant donné que je n'ai pas de carte à puce sur moi,
je vais utiliser un mot de passe.
Je crée un mot de passe que je tape deux fois.
C'est celui que je vais utiliser
pour déchiffrer le contenu de mon lecteur flash
à chaque fois que je connecte ce dernier à un ordinateur.
Quand c'est fait, une fenêtre s'affiche
et me demande comment enregistrer la clé de récupération.
Si vous perdez ce mot de passe ou votre carte à puce,
vous pouvez utiliser la clé de récupération pour accéder au lecteur
si c'est la méthode de déchiffrement sélectionnée.
Si vous n'avez pas très envie
de l'enregistrer dans un fichier sur un ordinateur,
vous pouvez toujours l'enregistrer dans un compte cloud.
Personnellement, je préfère l'imprimer et
la ranger en lieu sûr dans mon bureau.
Je clique sur Suivant
et j'obtiens une question difficile :
Voulez-vous chiffrer l'espace disque utilisé
ou voulez-vous chiffrer l'intégralité du lecteur flash ?
Si vous avez déjà supprimé des informations confidentielles
ou personnelles sur votre lecteur flash,
il est préférable de chiffrer l'intégralité du lecteur,
car si vous chiffrez uniquement l'espace disque utilisé,
seuls les fichiers se trouvant actuellement sur le lecteur sont chiffrés.
Mais, si vous avez supprimé des fichiers,
cet espace des fichiers supprimés
avec des outils d'analyse
sera récupéré
et ne sera pas chiffré.
Nous allons donc chiffrer l'intégralité du disque dur,
qui inclut l'espace vide et l'espace utilisé.
Étant donné que l'espace vide peut ne pas être vraiment vide,
car des fichiers supprimés ont pu s'y trouver,
je vais chiffrer l'intégralité du disque dur.
Maintenant, si j'utilise ce lecteur flash
sur plusieurs systèmes informatiques,
notamment différents systèmes d'exploitation Windows,
je veux m'assurer que j'utilise bien le mode compatible.

Si vous allez utiliser ce lecteur flash uniquement
sur les derniers systèmes Windows 10,
en passant d'un ordinateur à l'autre,
vous pouvez cliquer sur le nouveau mode de chiffrement
et ouvrir le lecteur sans problème.
En revanche, si vous essayez d'utiliser ce lecteur flash
avec ce nouveau mode de chiffrement,
qui correspond aux dernières versions de Windows 10,
il est possible qu'il ne soit pas compatible avec les autres systèmes d'exploitation
sur lesquels vous tentez d'ouvrir le lecteur.
Je vais donc choisir le mode compatible,
car il s'agit d'un lecteur flash USB que je vais
connecter à différents ordinateurs.
Lorsque cette option est sélectionnée, la fenêtre suivante vous indique
que vous pouvez déverrouiller le lecteur à l'aide du mot de passe que vous avez créé.
Je suis sur le point de le chiffrer,
je clique sur Démarrer le chiffrement.
C'est un petit lecteur flash.
Le processus peut être très rapide.
La taille est seulement de 256 Mo,
ce qui est parfait pour cette vidéo,
car avec un lecteur de 16 Go le processus prendrait du temps.
Pendant le chiffrement du disque,
vous pouvez voir des options en dessous.
Lorsque le chiffrement est terminé,
je peux enregistrer la clé de récupération,
modifier le mot de passe utilisé
ou supprimer complètement le mot de passe.
Je n'ai pas ajouté de carte à puce avant,
mais si je veux le faire
pour ouvrir le lecteur flash
et déchiffrer son contenu, je peux !
En plus, je peux
activer le déverrouillage automatique
du lecteur flash.
Enfin, je peux désactiver BitLocker,
qui déchiffrera définitivement l'intégralité du lecteur flash
et il ne sera plus possible de chiffrer mes fichiers sur ce lecteur.
Le chiffrement du lecteur E est terminé.
Je clique sur Fermer.
Regardons maintenant ce qui se passe.
Je viens d'éjecter mon lecteur flash USB de l'ordinateur
sur lequel BitLocker To Go est installé.
Je vais le rebrancher. Mon Explorateur de fichiers se trouve ici.

Regardez le premier message que j'obtiens :
« votre lecteur flash n'est pas accessible ».
Oh non, il est corrompu ?
Pas vraiment.
Je clique sur OK, et nous voyons
mon lecteur USB avec un verrou.
Je double-clique dessus et regardez le menu contextuel que j'obtiens.
BitLocker avec lecteur E.
Saisissez votre mot de passe pour le déverrouiller.
Je saisis mon mot de passe et je clique sur Déverrouiller,
et voilà ce qui se produit.
Il s'ouvre sur mon écran et
mes fichiers importants 1 à 5 sont là,
et maintenant tous les fichiers que je place ici,
avant d'éjecter le lecteur flash,
les nouveaux fichiers que j'ajoute ici,
vont être chiffrés à l'aide de BitLocker.
Voilà donc BitLocker To Go.
Revenons en arrière et passons à BitLocker
pour mon lecteur système fixe.
Ici, nous avons notre configuration BitLocker
avec notre lecteur flash USB chiffré.
Passons au lecteur de données fixe
où sont stockés le système d'exploitation
et les données elles-mêmes.
Nous voulons donc chiffrer ces données
du lecteur de système d'exploitation fixe.
Je clique sur Activer BitLocker
et j'obtiens un message d'erreur.
Il indique que l'appareil ne peut pas utiliser un TPM.
Un TPM est un module de plate-forme sécurisée.
Il s'agit de la puce sur la carte mère de notre système
utilisée pour le stockage matériel.
C'est là que nous aurons
les mots de passe et les clés sous forme de hashs, ainsi que les tris numériques.
Tout cela est stocké sur une puce TPM.
Si votre système n'est pas configuré pour utiliser ce type de stockage
ou s'il en est dépourvu, il existe d'autres moyens
d'utiliser BitLocker avec un logiciel.
Pour ce faire, je clique sur le bouton Démarrer,
je tape gpedit suivi de .msc
et nous avons ici Document de la console.
Et ce qui vraiment bien, c'est qu'un éditeur
s'ouvre en un clin d'œil

pour modifier les paramètres du système.
Pour moi, cet éditeur se trouve dans Modèles d'administration,
Composants Windows, et je clique sur
Chiffrement de lecteur BitLocker.
Maintenant, dans cette zone,
je vais accéder aux lecteurs du système d'exploitation,
et il y a l'option :
Exiger une authentification supplémentaire au démarrage.
Je double-clique dessus.
Et je clique sur Activé.
Je suis alors autorisé à utiliser le logiciel
pour chiffrer mon lecteur
et la clé n'est pas stockée sur une puce TPM.
Je clique ensuite sur Appliquer et OK.
Je ferme ensuite la fenêtre de l'Éditeur de stratégie de groupe,
puis je clique sur Activer BitLocker une deuxième fois,
et cette fois, il se charge.
Au lieu d'utiliser la puce TPM,
nous allons pouvoir stocker nos clés manuellement,
nous pouvons insérer un lecteur flash USB
pour que le contenu de ce lecteur soit déchiffré
ou alors utiliser un mot de passe.
Je ne veux pas utiliser un lecteur flash,
donc je clique sur Saisir un mot de passe.
Je choisis le mot de passe qui sera utilisé
pour déchiffrer l'intégralité du disque dur de mon ordinateur.
Je clique sur Suivant.
Tout comme nous l'avons vu précédemment avec le lecteur flash
et BitLocker To Go, nous pouvons choisir une méthode
de récupération du mot de passe en cas de perte.
De nouveau, je souhaite l'imprimer
pour le garder dans un coffre dans mon bureau.
Je clique sur Suivant.
Comme nous l'avons vu précédemment avec le lecteur flash, j'ai le choix entre
Chiffrer uniquement l'espace disque utilisé,
qui correspond à l'espace occupé par les fichiers sur le disque dur,
ou Chiffrer l'intégralité du disque, y compris l'espace libre
où pouvaient se trouver les fichiers supprimés.
Je choisis Chiffrer l'intégralité du disque.
À présent, pour des raisons de temps dans la vidéo,
comme il s'agit d'un disque dur,
je vais utiliser l'espace disque utilisé uniquement
pour accélérer les choses.
À nouveau, concernant les modes de compatibilité,

je n'envisage pas de sortir mon disque dur fixe
de la tour de mon ordinateur ou de mon ordinateur portable
pour le placer dans un autre système.
Donc je conserve le mode de chiffrement le plus approprié
qui est le nouveau mode de chiffrement pour les disques fixes.
Je clique sur Suivant.
Maintenant, je peux activer l'option de vérification du système,
qui garantit
que je peux utiliser correctement les clés de récupération
avant de chiffrer le disque entier.
Imaginez
que vous chiffriez votre lecteur
sans vous assurer que vous pourrez le déchiffrer.
Ce serait
risqué.
Il vaut donc mieux activer cette option par précaution.
Ensuite, je clique sur continuer.
J'obtiens alors une fenêtre contextuelle
qui m'indique de redémarrer l'ordinateur.
Reprenons la vidéo après le redémarrage.
L'ordinateur redémarre.
Je vois la page d'accueil du BIOS et BitLocker apparaît instantanément !
Je dois saisir mon mot de passe pour déverrouiller ce lecteur.
Tant que je ne l'ai pas fait, mon disque dur restera chiffré
et les données seront inaccessibles.
Je saisis donc mon mot de passe ici,
j'accède alors à l'écran de chargement de Windows
et je reviens à mon bureau.
Voici ce que nous avions à dire sur BitLocker To Go
et sur BitLocker pour notre lecteur fixe.
Merci de votre attention.
Exercez-vous et utilisez ce puissant outil,
et devenez un vrai pro de l'IT.