

- [Instructeur] Bonjour tout le monde.

Nous allons découvrir comment protéger notre système contre les virus.

Contre les virus et les programmes malveillants.

Pour commencer, le meilleur moyen de procéder

est de faire un clic droit sur le bouton Démarrer,  
puis de cliquer sur Paramètres dans Windows 10.

Lorsque la fenêtre Paramètres s'ouvre, je fais défiler l'écran vers le bas  
jusqu'à ce que je trouve Mise à jour et sécurité.

Lorsque je clique sur Mise à jour et sécurité,  
j'obtiens de nombreuses options  
pour protéger le système.

La première que je vois est Windows Update.

Et ce que vous pouvez faire de mieux pour protéger votre système,  
quel que soit le système d'exploitation utilisé,  
est de le mettre à jour.

De nombreux virus, programmes malveillants,  
et exploits courants peuvent être évités  
en mettant votre système à jour

avec les derniers Service Packs et les dernières mises à jour système.

Ils permettent au système de mieux fonctionner  
et le protègent contre certains des exploits  
qui le visent spécifiquement.

En dehors de Windows Update, je vais également examiner Sauvegarde.

Nos solutions antivirus ne peuvent pas empêcher  
tous les virus connus dans le monde entier.

Certains de ces virus sont nouveaux, ils sont de type « zero day »  
et nos antivirus ne les ont pas encore détectés,  
ils ne peuvent donc pas les bloquer.

Si votre système est infecté  
ou s'il est verrouillé par un ransomware,  
ce que vous pouvez faire,  
c'est de le restaurer à partir d'une sauvegarde.

Pour cela, vous devez disposer d'une sauvegarde.

Par conséquent, veillez à utiliser les sauvegardes  
de votre système d'exploitation, quel qu'il soit,  
afin de pouvoir le restaurer  
s'il est infecté.

Pour empêcher une infection  
de se produire,

je vais accéder à Sécurité Windows.

Sécurité Windows est, bien sûr,  
spécifique à Windows 10,

mais si vous utilisez un autre système d'exploitation,  
vous pouvez appliquer des mesures

de sécurité avec un antivirus  
et les paramètres dont je vais parler maintenant.  
Dans un premier temps,  
je clique sur Sécurité Windows  
et nous allons examiner l'antivirus.  
Lorsque la fenêtre Sécurité Windows s'ouvre,  
nous privilégions l'antivirus, car nous estimons que c'est ce qui compte le plus.  
Je vais donc d'abord  
cliquer sur Protection contre les virus et les menaces.  
Votre antivirus n'est efficace  
que si vous l'avez mis à jour  
avec les dernières définitions.  
Vous devez donc veiller à ce que votre système antivirus  
soit constamment à jour afin de détecter les menaces les plus récentes.  
Il y a des antivirus qui s'exécutent  
une fois seulement, lorsque vous cliquez sur Analyser  
et des systèmes antivirus  
qui analysent en permanence chaque fichier  
et application exécutés sur votre ordinateur.  
Il y a différentes façons de procéder.  
Vous pouvez utiliser les mises à jour de votre antivirus  
et même mettre à jour des options spécifiques  
pour empêcher les ransomwares de gâcher votre journée.  
En dehors de la protection contre les virus et les menaces  
pour assurer la sécurité de votre système,  
nous allons également parler du pare-feu.  
Tous les systèmes d'exploitation doivent disposer d'un pare-feu  
opérationnel, au moins sous forme logicielle.  
Avec votre pare-feu,  
vous autorisez les connexions à accéder à votre machine,  
et vous autorisez votre machine à accéder  
à des sites et des cibles spécifiques sur le web,  
et à recevoir des réponses.  
Les applications que vous installez qui utilisent Internet  
vont probablement demander une brèche dans votre pare-feu.  
Si vous supprimez un grand nombre d'applications  
et voulez rétablir les paramètres par défaut de votre pare-feu,  
cliquez sur des liens comme  
« Restaurer les paramètres par défaut des pare-feu »,  
et les paramètres par défaut du pare-feu  
sont rétablis. Débarrassez-vous aussi  
des applications tierces qui accèdent à Internet.  
À présent, en dehors du pare-feu, nous pouvons accéder au  
Contrôle des applications et du navigateur.

Pour bloquer les programmes malveillants  
tels que les chevaux de Troie,  
ou les malwares qui se font passer pour un autre programme,  
comme un économiseur d'écran inoffensif.  
Et lorsque vous l'exécutez, il installe un virus.  
Il est possible d'y remédier ici,  
par exemple avec l'option Vérifier les applications et les fichiers.  
Vous pouvez faire en sorte que votre système vous protège mieux  
en ne vous laissant pas télécharger des applications non reconnues,  
en les bloquant ou en vous avertissant  
avant l'exécution d'une application ou d'un fichier.  
C'est un moyen de protection supplémentaire.  
Voici quelques options courantes que vous pouvez utiliser  
pour sécuriser votre système  
et bloquer les programmes malveillants ou les virus  
qui pourraient vraiment gâcher votre journée.  
Merci d'avoir regardé la vidéo.  
Entraînez-vous avec les paramètres de sécurité  
et devenez un vrai pro de l'IT.