La sécurité. Directement intégrée.

Les puissantes technologies intégrées à OS X conjuguent en permanence leurs efforts pour examiner, chiffrer, mettre à jour et, au bout du compte, protéger votre Mac.

Gatekeeper. Téléchargez vos apps encore plus sûrement.

Gatekeeper s'assure que vous n'installez pas de logiciels malveillants par mégarde lorsque vous téléchargez des apps sur votre Mac. L'endroit le plus sûr pour télécharger des apps pour votre Mac est encore le Mac App Store. Apple passe chaque app en revue avant qu'elle soit acceptée par le Store, et si une app présente le moindre problème, Apple peut rapidement la retirer du Store. Gatekeeper sécurise également tous vos téléchargements de logiciels sur Internet, peu importe leur provenance. Apple fournit aux développeurs un identifiant Developer ID unique qui leur permet de signer numériquement leurs apps. Grâce à cet identifiant, Gatekeeper peut bloquer les apps conçues par des développeurs malveillants et s'assurer que les apps n'ont pas été falsifiées. Et il peut protéger votre Mac en empêchant l'installation d'apps conçues par des développeurs inconnus, qui ne sont pas identifiés par un Developer ID.

Gatekeeper vous procure davantage de contrôle sur ce que vous installez.

Gatekeeper vous offre trois options de sécurité. Vous pouvez télécharger et installer des apps provenant de partout sur Internet, opter exclusivement pour celles provenant du Mac App Store, la source de téléchargement la plus sûre pour votre Mac, ou utiliser l'option par défaut, qui vous permet d'installer les apps du Mac App Store et de développeurs identifiés par un Developer ID. Lorsqu'une app ne porte pas de signature numérique, Gatekeeper empêche son installation et vous informe qu'elle ne provenait pas d'un développeur approuvé. Si vous êtes certain que l'app est fiable, vous pouvez manuellement passer outre Gatekeeper en faisant un Contrôle-clic sur l'app et en choisissant de l'ouvrir.

Les mises à jour logicielles veillent sur votre Mac.

La meilleure façon de protéger votre Mac est de vous assurer que vos logiciels sont à jour. Et avec OS X Mountain Lion, cela devient plus simple que jamais. Il unifie les mises à jour des apps du Mac App Store et celles d'OS X. Lorsque de nouvelles mises à jour sont disponibles, Mountain Lion vous envoie une notification. Il suffit d'accepter les mises à jour d'un clic, et elles se téléchargent automatiquement. OS X vérifie désormais tous les jours s'il y a de nouvelles mises à jour. Il est donc très simple d'avoir toujours la version d'OS X la plus récente et la plus sûre.

La technologie du bac à sable isole le code malveillant.

App Sandbox, la technologie du bac à sable d'OS X, veille à ce que les apps ne fassent que ce qu'elles sont supposées faire. Elle isole les apps des composants système critiques de votre Mac, de vos données et de vos autres apps. Si une app contient du code malveillant, Sandbox la bloque automatiquement pour protéger votre ordinateur et son contenu. Sous OS X Mountain Lion, Sandbox offre une protection inégalée pour naviguer dans Safari en toute sécurité. Cette protection est également intégrée à de nouvelles apps comme Notes, Rappels et Game Center, et à des apps existantes comme Mail et FaceTime.

Protections d'exécutions. Au cœur même du système.

Les protections d'exécutions techniquement sophistiquées d'OS X Mountain Lion sont appliquées au cœur même de votre Mac pour mieux le protéger. Intégrée directement au processeur, la fonctionnalité XD (execute disable) établit une distinction nette entre la mémoire utilisée pour les données et celle utilisée pour les instructions exécutables. Votre Mac est ainsi protégé contre les logiciels malveillants qui pourraient tenter de l'amener à traiter des données de la même façon qu'il traite un programme et ainsi compromettre votre système. La technique ASLR (Address Space Layout Randomization, distribution aléatoire de l'espace d'adressage) modifie les emplacements dans la mémoire où les différentes parties d'une app sont stockées. Ceci complique la tâche à quiconque pourrait chercher à vous nuire en localisant puis en réorganisant les composants d'une app afin que celle-ci effectue des opérations qu'elle n'est pas censée effectuer. Mountain Lion applique la technique ASLR à la mémoire utilisée par le noyau au cœur d'OS X afin de protéger votre Mac de part en part.

Antiphishing. Les sites frauduleux ne lui disent pas merci.

Le phishing est une forme d'attaque en ligne visant à récupérer des informations sensibles telles que des noms d'utilisateur, des mots de passe et des informations de carte bancaire, en créant de faux sites web qui ressemblent à ceux de véritables entreprises — comme le site de votre banque ou d'un réseau social. La technologie antiphishing de Safari vous protège de telles attaques en détectant ces sites web frauduleux. Et si vous essayez d'accéder à un site suspect, Safari désactive la page et affiche une alerte.

FileVault 2 chiffre vos données.

Avec FileVault 2, vos données sont en sécurité. Même si elles tombent entre de mauvaises mains. FileVault 2 chiffre tout le contenu de votre Mac et protège vos données grâce au chiffrement XTS-AES 128. Le chiffrement initial est rapide et discret. FileVault 2 peut également chiffrer des disques amovibles, afin de sécuriser vos sauvegardes Time Machine et autres disques externes. Vous voulez repartir à zéro ou donner votre Mac à quelqu'un ? FileVault 2 permet d'en effacer les données facilement. L'effacement instantané supprime la clé de chiffrement de votre Mac — ce qui rend les données totalement inaccessibles — puis s'applique à effacer méthodiquement toutes les données du disque.

Votre Mac veille au grain.

Des fichiers en apparence inoffensifs téléchargés d'Internet peuvent dissimuler des logiciels malveillants. C'est pourquoi les fichiers téléchargés à l'aide de Safari, Mail et Messages sont vérifiés en détail pour voir s'ils contiennent des applications. Si c'est le cas, OS X vous avertit, puis vous prévient la première fois que vous ouvrez une application. À vous de décider si vous voulez ouvrir l'application ou non. Et si un fichier contient un logiciel identifié comme étant malveillant, OS X propose de le placer dans la corbeille.

Le Contrôle parental protège vos petits.

En tant que parent, vous souhaitez que vos enfants profitent d'Internet en toute sécurité et en évitant les mauvaises surprises. OS X veille. À l'aide de simples réglages dans le volet Contrôle parental, vous pouvez gérer le temps que vos enfants passent sur le Mac, les sites qu'ils consultent et les personnes avec lesquelles ils communiquent.

OS X. Des mots de passe encore plus fiables.

OS X vous permet de profiter d'Internet en toute sécurité, que ce soit pour consulter votre compte bancaire, envoyer des messages confidentiels ou partager des fichiers avec amis ou collègues. Des fonctionnalités telles que l'Assistant mot de passe vous aident à créer des mots de passe plus sûrs pour déjouer les usurpateurs d'identité, tandis que les technologies de chiffrement intégrées vous aident à protéger vos informations personnelles et vos communications.

Les réglages de confidentialité protègent votre vie privée.

Les Préférences Système contiennent désormais des réglages de confidentialité qui permettent de gérer le partage de la localisation et des informations de diagnostic. Les préférences de Safari proposent elles aussi des options de confidentialité qui vous permettent de limiter ou de bloquer l'utilisation des cookies et de limiter l'accès des sites web aux services de localisation. Safari propose également un paramètre indiquant aux sites web de ne pas surveiller vos activités de navigation.

OS X et iCloud vous aident à retrouver votre Mac égaré.

OS X et iCloud peuvent vous aider à protéger votre Mac même quand vous ne savez plus où vous l'avez mis. Connectez-vous à iCloud.com à partir d'un autre ordinateur ou utilisez l'app Localiser mon iPhone sur un iPhone, iPad ou iPod touch pour localiser sur une carte votre Mac égaré. Si votre Mac est hors ligne lorsque vous essayez de le retrouver, vous pouvez demander à recevoir un e-mail dès qu'il établit une connexion Wi-Fi. Vous pouvez également afficher un message sur l'écran de votre Mac pour indiquer à la personne qui l'a trouvé comment vous le rendre. Mieux encore : en attendant de récupérer votre Mac, vous pouvez effectuer un verrouillage par mot de passe ou même supprimer à distance vos données personnelles et rétablir les réglages d'origine.

Des mesures supplémentaires pour protéger votre Mac.

Bien qu'aucun système ne puisse être immunisé à 100 % contre toutes les menaces, OS X vous permet d'en faire plus pour protéger au mieux vos informations. Vous trouverez la plupart de ces fonctionnalités de sécurité supplémentaires dans le volet Sécurité et confidentialité des Préférences Système. Voici quelques-unes des mesures que vous pouvez prendre :

- Activez un pare-feu afin d'empêcher d'autres ordinateurs d'accéder aux services qui tournent sur votre Mac.
- Contrôlez l'accès à votre Mac en verrouillant votre écran après un délai d'inactivité.
- Supprimez en toute sécurité les fichiers confidentiels devenus inutiles au moyen de la commande Vider la corbeille en mode sécurisé.
- Configurez le partage de fichiers sécurisé.