L'assurance en plus facile.

Mobilisés pour nos partenaires

Se protéger des cyberrisques lorsqu'on travaille à domicile

L'épidémie de COVID-19 et les mesures sans précédent prises par les autorités dans de nombreux pays du monde obligent les entreprises à adapter leurs méthodes et outils de travail. Cette situation, qui sort de l'ordinaire à l'échelle internationale, offre de multiples opportunités aux pirates informatiques pour mener des attaques contre les entreprises : c'est une cyber-menace que nous prenons très au sérieux, et que nous pouvons combattre ensemble en adoptant les bons réflexes.

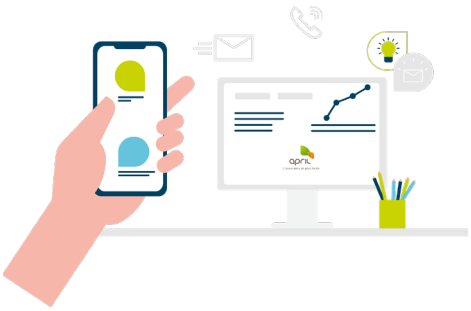
Nous avons identifié deux des types d'attaques les plus courantes - dont nous constatons une augmentation ces derniers jours - et nous vous apportons les réponses aux questions que vous vous posez :

Le vol d'identité

Il s'agit de tentatives d'usurpation de l'identité d'un dirigeant, d'un membre de votre comité exécutif ou d'un fournisseur pour obtenir la réalisation de transactions financières sans respecter la gouvernance et les procédures habituelles, sous prétexte d'urgence. Ces usurpateurs sont très bien informés et préparés, ce qui rend leurs techniques très efficaces. Ces tentatives peuvent être effectuées par téléphone ou par courrier électronique. N'oubliez pas qu'aucun des dirigeants de votre groupe ne vous contacterait directement pour effectuer des opérations financières confidentielles sans respecter les procédures en vigueur. En tout état de cause, si vous recevez une sollicitation inhabituelle concernant une opération financière ou la récupération de données sensibles, vérifiez systématiquement auprès de votre Direction et/ou de vos équipes financières.

Aucun des dirigeants de votre groupe ne vous contacterait pour effectuer des opérations financières confidentielles sans respecter les procédures en vigueur

Applications et sites malveillants



En prétendant diffuser des informations relatives à COVID-19, les pirates informatiques peuvent vous conduire vers des applications et/ou des sites malveillants susceptibles d'aspirer vos données ou d'introduire des virus dans votre système: nous vous invitons à être doublement vigilants avant de cliquer sur un lien ou d'installer une application et à vous limiter aux sources d'information officielles. La prudence et le bon sens sont une aide précieuse dans ce type de situation. Nous souhaitons attirer votre attention sur le fait que l'utilisation massive du télétravail pourrait entraîner une augmentation de ces tentatives de fraude.

Le travail à domicile offre de multiples opportunités aux pirates informatiques.

Quelques bonnes pratiques pour travailler à distance

- N'oubliez pas de travailler dans un endroit qui peut être isolé et de verrouiller votre poste de travail après utilisation. Il se peut que vous ayez à manipuler des informations sensibles qui ne sont pas accessibles à votre entourage.
- N'utilisez votre équipement professionnel qu'à des fins professionnelles et n'essayez pas d'y installer quoi que ce soit.
- Si vous vous connectez à votre PC via le wifi, vérifiez qu'il est sécurisé par une clé secrète, et si ce n'est pas le cas, activez le cryptage, déconnectez et reconnectez votre ordinateur.
- Si d'autres appareils de votre famille sont connectés à votre réseau domestique et à votre boîtier, assurez-vous qu'ils sont équipés d'un logiciel antivirus avec une base de données de signatures à jour, que les systèmes d'exploitation des ordinateurs sont à jour avec les correctifs de sécurité et que la fonction de mise à jour automatique est activée ; et effectuez régulièrement des analyses de virus sur ces appareils pour vous assurer qu'ils ne risquent pas d'infecter tous les appareils connectés à votre réseau domestique et à votre boîtier.
- Accédez à vos applications via le VPN et les solutions de protection mises en place sur le réseau. N'oubliez pas de vous déconnecter de la session VPN une fois votre travail terminé (après avoir copié vos fichiers dans les zones du réseau).
- Ne connectez pas vos équipements personnels (imprimante, disques externes) à votre PC.
- Si votre PC se comporte de manière anormale, veuillez le déconnecter du réseau ; ne vous connectez plus au VPN et demandez de l'aide afin de faire vérifier l'état de votre ordinateur.
- Ne cliquez pas sur des liens ou des pièces jointes provenant de personnes non vérifiées.
- Méfiez-vous de tout courrier électronique faisant référence au Coronavirus ou au COVID-19