www.groupe2b.com



COVID 19

FICHE ALERTE SECURITE CYBERATTAQUE

La crise du coronavirus : nouveau terrain de jeu des pirates informatiques !

POURQUOI EN CE MOMENT ?

> Parce que les conditions de travail que nous vivons (télétravail, réduction d'effectif, ...) sont inhabituelles et peuvent être déstabilisantes ;

> Parce que l'ambiance anxiogène liée à la gestion de crise peut induire des comportements à risque ;

> Parce que des attaquants profitent de l'actualité pour générer des escroqueries ou des actes malveillants ;

QUELLES SITUATIONS A RISQUES ?

> Mise en ligne de **fausses** attestations de déplacement sans limite de date, dans le but de collecter des données personnelles ou de vous demander de l'argent ;

> Déploiement de logiciels malveillants (type rançongiciels (« ransomware »)) via de **fausses** applications pour smartphone, censées suivre l'évolution du virus ;

> En se faisant passer pour la collectivité, l'assistance informatique ou la DRH, ou en demandant d'appeler un **faux** numéro, en prétextant un problème informatique ou une directive RH, dans le but de bloquer votre ordinateur, votre smartphone, ou de vous soutirer de l'argent ;

> En utilisant la technique habituelle de l'hameçonnage (« phishing ») pour prendre une **fausse** identité officielle (site du ministère de la santé par exemple), afin de vous faire cliquer sur un lien frauduleux dans un mail ou SMS..

Suivez-nous !

QUE FAIRE POUR REDOUBLER DE VIGILANCE FACE A CES APPELS / MESSAGES ?

> Vérifiez l'identité de leur expéditeur, en cas de doute, supprimez le mail et appelez vos contacts habituels ;

> Ne cliquez surtout pas sur les liens qui vous paraissent suspects (en particulier si vous ne reconnaissez pas l'adresse Internet (URL) qu'ils indiquent) ;

> Ne vous connectez que sur des sites officiels (ceux qui se terminent par « seinemaritime.fr » ou « gouv.fr » par exemple), et ne cliquez pas sur les liens présents dans les mails, utilisez plutôt le moteur de recherche de votre navigateur Internet (exemple : https://qwant.fr) ;

> Ne propagez pas de tels messages, et n'alertez pas la cellule d'assistance informatique (sauf en cas de récidive ou si vous êtes confrontés à un blocage), mais supprimez-les immédiatement ;

> N'installez pas d'applications gratuites, elles sont potentiellement porteuses de code malveillant ;

> Ne communiquez jamais votre mot de passe à quiconque, et verrouillez votre ordinateur quand vous sortez ;

> Ne communiquez jamais de données personnelles à quiconque ou sur aucun site sans en avoir vérifié la source ;

> En télétravail, protégez le matériel contre le vol, et ne mélangez pas vie privée et vie professionnelle ;

> Ne connectez pas de périphériques de stockage externe (clé USB par exemple) à votre ordinateur.

ET SURTOUT ...

Si vous pensez être victime d'une attaque, déconnectez-vous immédiatement, et contactez assistance informatique.

CONCLUSION :

La période de crise est une opportunité supplémentaire pour les pirates informatiques. Ces attaques sont réelles ! – RESTONS VIGILANTS !

La responsabilité du Groupe 2B ne pourra pas être engagée au titre des informations contenues dans cette note établie à titre informatif et susceptible d'évoluer d'heure en heure en fonction des annonces gouvernementales.