LES HACKERS SONT CONFINÉS MAIS NE SONT PAS AU CHOMAGE PARTIEL !

Chers Assurés,

Le contexte d'angoisse et de stress lié au Coronavirus rend les pirates informatiques plus audacieux que les mois derniers.

Les cybercriminels cherchent à tirer profit de la précipitation et de la baisse de vigilance des utilisateurs pour les abuser.

Nous vous joignons une plaquette d'information sur des cybers attaques depuis 2018.

Ces actes malveillants sont amplifiés par l'accroissement de l'usage numérique lié aux mesures de confinement.

Le basculement dans le télétravail de 8 millions de Français a été fait dans l'urgence, malheureusement au détriment de la sécurité informatique. Beaucoup de télétravailleurs utilisent des plateformes non sécurisées et ça les hackers l'ont bien compris !

Par ailleurs, les fournisseurs internet ont répertorié une augmentation **de 667 % du nombre d'attaques par phishing, dans le monde.**

Médirisq - Sauret Célia - le 17/04/2020

Les hackers utilisent le thème du Covid-19 pour appâter leurs cibles avec des mails émanant de l'Organisation Mondiale de la Santé sur la prévention des virus, ou des mails proposant des achats de masques chirurgicaux et au du gel hydroalcoolique.

LA VENTE DE MASQUES CHIRURGICAUX EST INTERDITE EN FRANCE. Ces équipements font l'objet d'un réquisitionnement de l'Etat et leur diffusion auprès des particuliers est soumise à la délivrance d'une ordonnance médicale.

DONC TOUS LES SITES DE VENTE SONT FRAUDULEUX !

Si vous avez effectué une commande sur un tel site contactez votre banquier afin qu'il surveille les mouvements sur votre compte.

Par ailleurs, depuis les annonces gouvernementales sur les aides aux entreprises, les mails frauduleux revêtissent la tenue bleue, blanc et rouge de la République Française pour vous annoncer une régularisation financière émanant du Trésor Public (cf exemple ci-dessous).

Il faut être prudent car le but des cybercriminels étant de voler des informations d'identification pour **escroquer de l'argent aux utilisateurs**.

Quelques gestes simples :

1. **Toujours être suspicieux dès la réception d'un mail**
2. **Vérifiez l'orthographe, la grammaire cela peut vous mettre la puce à l'oreille (ex : Crise sanitaire « sang » précédent)**
3. **Afficher l'adresse mail de l'expéditeur (ex : …..@tokyo.com)**
4. **Ne cliquez sur aucun lien contenu dans le mail**
5. **N'ouvrez pas les pièces jointes**
6. **Ne répondez pas au mail**
7. **Classez-le dans vos courriers indésirables**
8. **Vous pouvez toujours appeler directement l'établissement censé vous contacter, chercher soi-même le numéro du service client afin de vérifier l'authenticité de la demande (/ ! \ ne pas utiliser le téléphone sur le mail / ! \ )**

Les cibles préférées des pirates sont les professionnelles de santé, nous vous invitons donc à redoubler de vigilance et ne vous laisser pas entrainer par les chants des sirènes des Cyber attaques.

L'ANSSI a répertorié **18 attaques par rançongiciels dans le secteur de la santé.** Toutefois, il demande des investissements dans la sécurité informatique des acteurs de la santé. « *Cette densité d'attaques résulte d'un sous-investissement chronique en sécurité informatique. Sous la contrainte budgétaire, le développement des applications a été privilégié à la sécurité Informatique* ». Les établissements ont été laissés « *à la merci d'attaquants pour lesquelles les entités, dont la rupture d'activité aurait un impact social important, sont des cibles intéressantes* ».

LES PIRATES NE S'ARRETENT PAS LA. Des sites frauduleux proposent des **attestations de déplacement dérogatoire** et des **justificatifs de déplacement professionnel** payants ou à remplir en ligne. La finalité étant de toujours vous dérober vos données personnelles. Nous vous rappelons que les attestations et justificatifs officiels sont **gratuitement téléchargeables** sur le site du ministère de l'Intérieur : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Attestation-de-deplacement-et-de-voyage

Il est donc primordial de redoubler d'attention pour ne pas tomber dans leurs pièges.

Si vous avez le moindre doute n'hésitez pas à nous consulter, nous sommes là pour vous aider.

Médirisq - Sauret Célia - le 17/04/2020

Vous pouvez également consulter le site du gouvernement sur la cyber malveillance afin d'obtenir plus d'informations : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite

LES CYBERCRIMINELS NE REDOUTENT PAS LE VIRUS, ILS LE FABRIQUENT !!

Prenez soin de vous et de vos proches, et restez vigilants,

Bien cordialement.