COVID-19 Le risque cyber sécurité s'intensifie.

Vol de données personnelles, bancaires, fuite de données confidentielles, indisponibilité de systèmes indispensables à la gestion de la crise sanitaire... **Les impacts pourraient être critiques.**

CHU AMIENS PICARDIE

La pandémie que nous vivons **augmente** considérablement le **risque cyber sécurité** :

> Les **acteurs malveillants** profitent de l'inquiétude générée pour diffuser de **fausses informations, malwares et arnaques** en tout genre.

> La généralisation du **télétravail**, qui n'a pas nécessairement pu être préparé de façon **sécurisée**.

Applications et sites malveillants

Cette carte de propagation du Covid-19 contient un spyware qui permet de récupérer des mots de passe, numéros de cartes bancaire ou autres données confidentielles. D'autres applications verrouillent le téléphone et exigent une rançon.

Phishing

E-commerce frauduleux

Ventes de masques, de gel hydroalcoolique, de médicaments miracles ou de vaccins expérimentaux, faux appels au dons ou autres «fake news» : de nombreuses arnaques voient le jour.

Les entreprises (public / privé), hopitaux, etc., sont aussi ciblés

Un hôpital tchèque frappé par une cyberattaque en pleine épidémie de COVID-19

Technologie : L'un des plus grands laboratoires d'essais sur le COVID-19 de la République tchèque frappé par une mystérieuse cyberattaque.

ZDNet Par Catalin Cimpanu | Modifié le samedi 14 mars 2020 à 10:00

Coronavirus : une société pharmaceutique escroquée de 6,6 millions d'euros

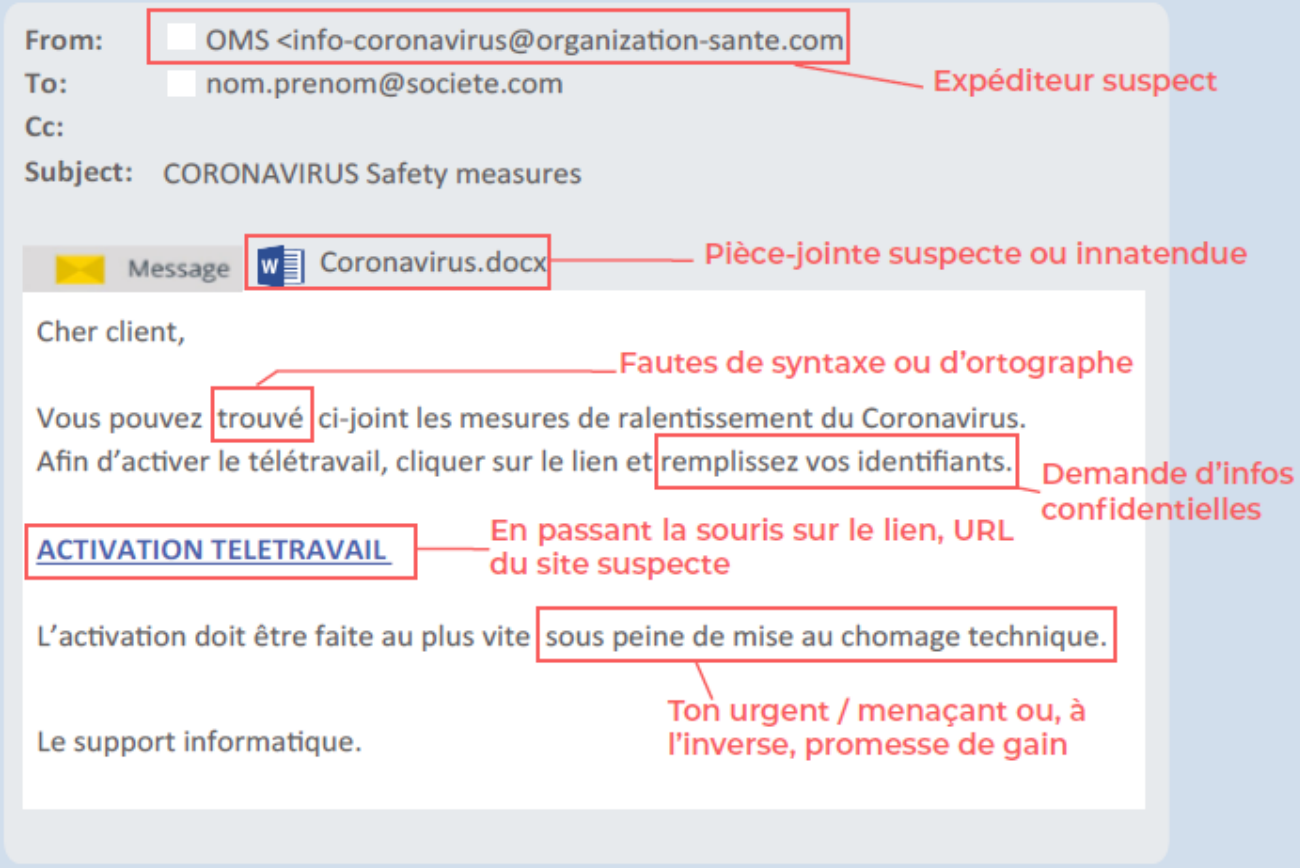
Une entreprise pharmaceutique de Rouen avait passé une commande massive de masques et de gels à une société qui s'est révélée fausse. Une enquête a été ouverte.

Les hackers sont agiles : peu de temps après la mise en place des autorisations de sortie, des sites et applications malveillants proposant de remplir les autorisations sont créés : **attention aux vols de données et malwares !**

Comment se protéger ?

Vigilance face au phishing

Le phishing est une **attaque** visant à récupérer des **informations confidentielles** (mot de passe, information bancaire,...) ou à **implanter un malware** sur le PC.



CHU AMIENS PICARDIE

D'autres éléments peuvent avertir d'un phishing : Sujet inhabituel, esthétique ou agencement douteux, e-mail non / mal personnalisé...

J'ai un doute sur la légitimité d'un e-mail...

- Ne pas transférer l'e-mail à des collègues.
- Ne pas ouvrir les PJ et ne pas cliquer sur les liens.
- Refuser de donner des mots de passe ou des infos confidentielles (même au support informatique).
- Alerter le support informatique puis supprimer l'e-mail.

Télétravailler de façon sécurisée

Utiliser une connexion sécurisée
Utilisez le VPN pour accéder au réseau de l'entreprise (via votre box internet ou téléphone). Évitez l'utilisation des réseaux Wifi public qui peuvent être piratés : vos données peuvent être interceptées et / ou modifiées.

Séparer les usages pro et perso
Verrouillez votre poste afin d'éviter les modifications ou suppressions malencontreuses. Votre poste professionnel ne doit pas être utilisé par votre entourage (enfants par exemple). L'usage personnel doit être restreint afin de limiter les risques de piratage et de surcharge du réseau de l'entreprise.

Sauvegarder ses documents
De façon régulière, sauvegardez vos documents sur le serveur de fichier ou l'espace de stockage Cloud de l'entreprise afin d'éviter toute perte de données. Evitez d'utiliser des clés USB personnelles : elles sont un vecteur important de fuite de données.

Assurer la protection du matériel
En télétravail comme dans les locaux de l'entreprise, pensez à appliquer les mises à jour de sécurité et à utiliser des mots de passe complexes : cela pourrait éviter une attaque. De même, le téléchargement sur internet est dangereux : contactez votre service IT si vous avez besoin de nouveaux logiciels / applications.

Être vigilant sur la navigation internet
Le surf internet est une source importante d'infection virale. Les malwares peuvent infecter votre poste lors de la consultation de sites qui se sont fait pirater, de sites non sûrs ou illicites (sites de jeux, de contrefaçons, de téléchargement...). Méfiez-vous des belles occasions : par e-mail ou sur internet.

Votre poste a un comportement anormal ?
Vous pensez avoir cliqué sur un phishing ?
En cas de doute, n'hésitez pas à contacter le support informatique ou l'équipe sécurité.

Sources :
https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware
https://threatpost.com/working-from-home-covid-19s-constellation-of-security-challenges/153720/
https://www.bbc.com/news/technology-51838468
https://www.zdnet.fr/actualites/un-hopital-tcheque-frappe-par-une-cyberattaque-en-pleine-epidemie-de-covid-19-39900659.htm
https://nakedsecurity.sophos.com/2020/03/19/ddos-attack-on-us-health-agency-part-of-coordinated-campaign/

CHU AMIENS PICARDIE

La Direction des Services Numériques et son support informatique : 14000 ou 03 22 08 81 08

L'équipe cyber sécurité et conformité réglementaire RGPD en cas de violation de vos données personnelles : dpo@chu-amiens.fr