Campagne de sensibilisation sur la cybersécurité [COVID-19]

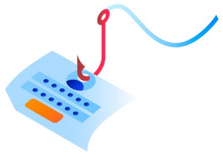
La pandémie du coronavirus est le sujet de préoccupation du monde entier en ce moment. Tous les jours, de nombreux nouveaux articles parlant du virus sont publiés : les moyens de protection contre la contamination, le nombre de personnes touchées dans chaque pays, le nombre de décès etc.

Les pirates informatiques profitent de cette situation et attaquent les utilisateurs d'outils informatiques par plusieurs moyens en exploitant ces thématiques qui tournent autour du COVID 19. Parmi les procédés d'attaque les plus répandus, existe ce qu'on appelle **le Phishing.**

Mais qu'est-ce que le Phishing ?

Le phishing, aussi appelé hameçonnage, est une technique de « social engeneering » qui a pour but de voler à des victimes leurs identifiants de connexion ainsi que leurs mots de passe ou encore leurs numéros de cartes bancaires. C'est parmi les procédés les plus simples qui arrivent à tromper les cibles.

La personne ciblée reçoit un email de la part d'un attaquant qui se fait passer par un fournisseur d'accès internet, une banque, ou encore une organisation de santé. Dans cet email, le pirate demande à la cible de mettre à jour ses informations bancaires ou encore ses identifiants de connexion. L'email comporte un lien dirigeant à une page qui semble sécurisée, et si la cible clique dessus et renseigne ses données personnelles, elle sera donc victime de l'attaque de phishing.



Se méfier des faux messages

Les faux messages les plus répandues au sujet du coronavirus sont :

- Des fausses offres de masques de protection,
- De fausses collectes de fonds pour les personnes malades,
- Des liens dirigeant vers de faux sites d'information,
- De fausses offres de vaccins.

Pour éviter les attaques de phishing, il faut :

- ✓ Se méfier des messages parlant du coronavirus,
- ✓ Ne pas cliquer sur les liens avant de réfléchir car ils peuvent contenir des virus qui seront téléchargés sur l'ordinateur,
- ✓ Eviter de communiquer ses données personnelles ou bancaires,
- ✓ Ne pas acheter des masques de protection sur des sites suspects ou suite à la réception d'un mail suspect,
- ✓ Faire attention à ne pas croire aux fausses informations.

Comment détecter et éviter les tentatives de phishing ?

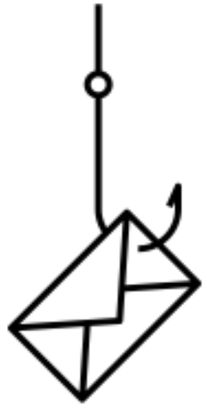
Il existe des indices qui permettent d'identifier les tentatives de phishing.

Les images : Les images floues des faux sites web ainsi que les images déformées sont un signe révélateur.

Le design : Le design des pages d'accueil des faux sites sont souvent différents ceux des sites officiels.

Une sensation d'urgence : Les sites web des pirates véhiculent des sensations d'urgence, ce qui pousse le visiteur à cliquer rapidement sur le lien.

Les fautes : la présence de fautes de frappe courantes est un autre signe révélateur de l'attaque de phishing.



Quelques bonnes pratiques supplémentaires de cyber sécurité que tout individu doit obligatoirement prendre en compte pour limiter les risques d'attaques et se protéger contre les hackeurs :

- Se méfier des emails de personnes inconnus
- S'assurer que la connexion Wi-Fi est assez sécurisée,
- S'assurer du fonctionnement et de la mise à jour de l'antivirus,
- Verrouiller son écran si l'on ne travaille pas dessus,
- Vérifier que les outils de chiffrement sont installés.

“ Mieux vaut prévenir que guérir... ”