Cybersécurité 401

Et la COVID-19

Introduction:

La pandémie de COVID-19 présente un éventail extraordinaire de défis en matière de cybersécurité

Étant donné que l'épidémie de COVID-19 surcharge le système de santé et l'économie mondiale, elle a également un impact puissant sur la sécurité des entreprises et des particuliers.

"Les fraudeurs saisiront toutes les opportunités qu'ils peuvent pour prendre de l'argent à des innocents.
Cela comprend l'exploitation des tragédies et des urgences mondiales«

a déclaré
le chef du National Fraud Intelligence Bureau.

Le nombre de rapports sur la cybercriminalité du FBI a quadruplé depuis le début de la pandémie

…

la plupart étant directement liés au Covid-19.

Google a révélé que chaque jour de la semaine dernière, ses systèmes informatiques liés à Gmail ont détecté - et bloqué –

18 millions de courriels d'hameçonnage liés au COVID-19

En plus de cela, Google a également bloqué plus de …

240 millions de messages indésirables quotidiens liés au virus.

Ainsi, les systèmes d'apprentissage automatique de Google,
étaient devenus si efficaces pour détecter les menaces en ligne
qu'il réussissait à empêcher 99,9%
du spam, du phishing et des logiciels malveillants
avant d'atteindre la boîte de réception Gmail.

Principales menaces générales

Hameçonnage par courriels et textos frauduleux

Logiciels malveillants

Vol d’identité

7 façons dont les pirates et les escrocs exploitent la panique du coronavirus

La plupart des cyberattaques actuelles exploitent principalement les craintes entourant l'épidémie de COVID-19 –

alimentées par:

- La désinformation
- Les fausses nouvelles et canulars
- Des leurres sur le thème des coronavirus

que les cybercriminels utilisent à des fins d'espionnage et de gain commercial.

Rob Lefferts, vice-président de Microsoft 365 Security.

Ces attaques représentent moins de 2% de toutes les attaques analysées quotidiennement par Microsoft.

"Nos données montrent que ces menaces sur le thème de COVID-19 sont des rechapes d'attaques existantes qui ont été légèrement modifiées pour être liées à cette pandémie"

"Cela signifie que nous assistons à un changement de leurres, et non à une augmentation des attaques."

1 – Malveillance pour les appareils mobiles (Mobile malware)

"Les acteurs qualifiés de la menace exploitent les préoccupations des gens concernant le coronavirus pour propager des logiciels malveillants mobiles,
y compris les chevaux de Troie d'accès à distance mobile et les appels robotisés,
via des applications qui prétendent offrir des informations et de l'aide aux utilisateurs sur le coronavirus"

2 – Hameçonnage par courriel (Email phishing)

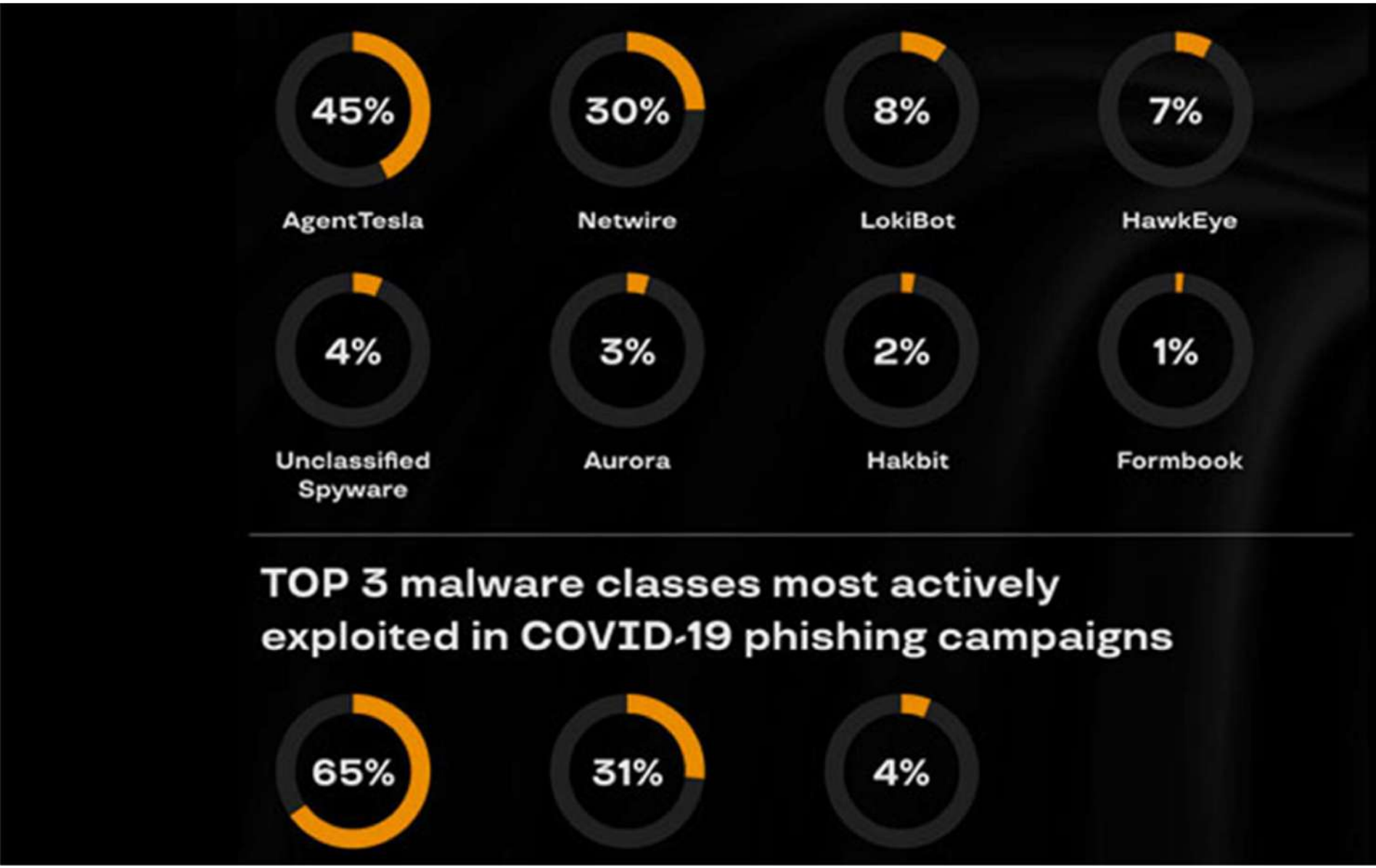
La plupart des courriels par hameçonnage liés à la COVID-19 étaient fournis avec:

- AgentTesla (45%)
- NetWire (30%)
- LokiBot (8%)

intégrés en pièces jointes, permettant ainsi à l'attaquant de voler des données personnelles et financières.

Suite ...

Les courriels, qui ont été envoyés
entre le 13 février et le 1er avril 2020,
se sont fait passer pour des avis de santé de
l'Organisation mondiale de la santé (OMS),
de l'UNICEF
et d'autres agences et sociétés internationales



TOP 3 malware classes most actively exploited in COVID-19 phishing campaigns

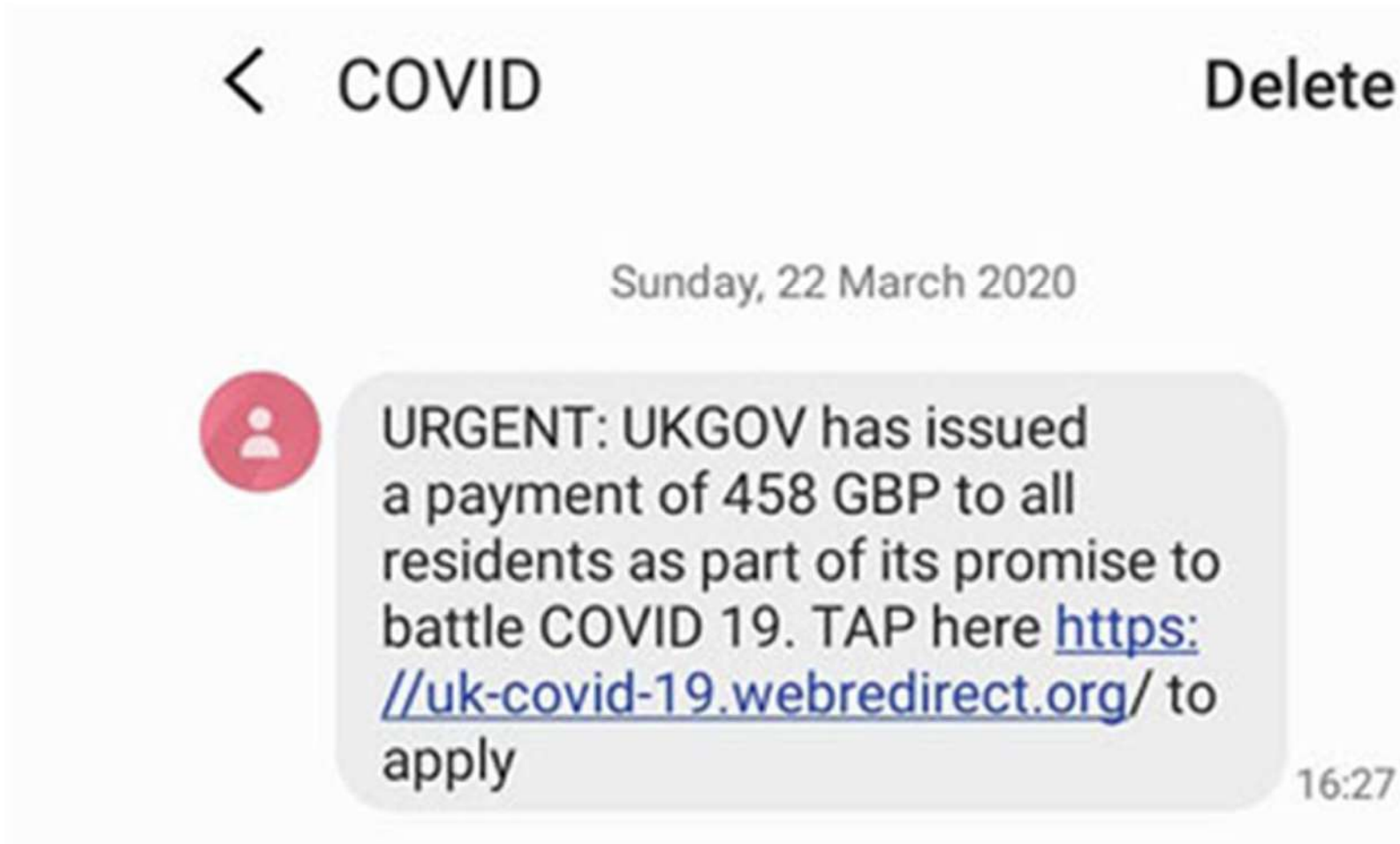
3 - Logiciels malveillants à prix réduit

Alors que le monde s'attaque à la pandémie du COVID-19, la situation s'est révélée être une bénédiction déguisée pour les acteurs de la menace, qui ont profité de l'occasion pour cibler les victimes avec des escroqueries ou des publicités de logiciels malveillants.

Les pirates informatiques exploitent la COVID-19 pour propager leurs propres infections, notamment en enregistrant des domaines malveillants liés au coronavirus et en vendant des logiciels malveillants à prix réduit sur le marché.

4 – Hameçonnage par message texte-texto (SMS Phishing)

De faux SMS provenant d'expéditeurs tels que « COVID » et « UKGOV » (United Kingdom Government)
qui contiennent un lien vers des sites d'hameçonnage (phishing).


COVID
Delete
Sunday, 22 March 2020
URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply
16:27

5 – Arnaque pour les masques et désinfectant pour les mains (Face Mask and Hand Sanitizer Scams)

Europol a récemment arrêté un homme de 39 ans originaire de Singapour pour avoir prétendument tenté de blanchir de l'argent généré par une escroquerie par courrier électronique en se faisant passer pour une entreprise légitime qui a annoncé la livraison rapide de masques chirurgicaux et de désinfectants pour les mains.

Une société pharmaceutique anonyme, basée en Europe, a été accusée d'une fraude sur 6,64 millions d'euros après que les articles n'aient jamais été livrés
et le fournisseur est devenu introuvable.

Home > All products > Antiviral N95 Mask For Anti Pollution...





Antiviral N95 Mask For Anti Pollution, Bacteria and Particulates with N95/N99 Filters

★★★★★ 4.9 (10 Reviews)

Color: Black

Black

Price: $24.99 ~~$64.99~~

& FREE Shipping

Stock: ● In stock

Quantity: 1

ADD TO CART

6 – Logiciels malveillants (Malicious Software)

Alors que les gens travaillent de plus en plus à partir de plates-formes de communication à domicile et en ligne telles que Zoom et Microsoft Teams, les acteurs de la menace envoient des courriels d'hameçonnage contenant des fichiers malveillants avec des noms tels que :

(n.d.l.r. à noter l'appellation fausse volontairement modifiée pour vous arnaquer)

"zoom-us-zoom _ ##########". Exe''

"microsoft-teams_V # mu # D _ ##########. exe "

… dans le but d'inciter les gens à télécharger des logiciels malveillants sur leurs appareils.

7 – Demande de rançon (Ransomware Attack)

Les cybercriminels tentaient de cibler les principaux hôpitaux et autres institutions en première ligne de la lutte contre le COVID-19 avec des rançongiciels :

« Les cybercriminels utilisent des ransomwares pour garder les hôpitaux et les services médicaux en otage numériquement, les empêchant d'accéder aux fichiers et systèmes vitaux jusqu'à ce qu'une rançon soit payée »

(n.d.l.r.: pas au Canada … encore!)

(mes) outils de protection et prévention pour optimiser les performances sur tous les appareils PC et mobiles

- Antivirus protection totale
- Antimalware
- Gestionnaire de mots de passe
- VPN (Virtual Private Network)
- Authentification à deux facteurs
- Mises à jour de Windows 10
- Mises à jour de Google
- Mises à jour de Samsung et Android (système d'opération)
- Mises à jour des applications, extensions, logiciels tiers
- Nettoyeurs de cache, de disques, stockage, fichiers temporaires, etc

Pourquoi?

Pour mettre toutes les chances de mon coté de ne pas être victime de cyberattaques

Pour rendre la tâche aux cybercriminels plus difficile

Et surtout pour éviter tous les problèmes personnels, sociaux et financiers liés au vol d'identité par exemple: Desjardins.

Fait parti de ma routine, mon hygiène et *ADN* informatique au quotidien

J'investis dans la prévention et l'optimisation de tous mes périphériques

2000 escrocs du coronavirus mis hors ligne lors d'une répression majeure d’hameçonnage

Par National Cyber Security Center (NCSC) Royaume Uni:

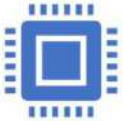
La pandémie de coronavirus a conduit à un nombre record d'organisations obligeant les gens à travailler à domicile - et dans de nombreux cas, ces employés n'ont aucune expérience préalable du travail à distance et pourraient ignorer certains des risques de sécurité potentiels:

471 fausses boutiques en ligne vendant des articles frauduleux liés aux coronavirus
555 sites de distribution de logiciels malveillants
200 sites d’hameçonnage
832 fraudes sur les frais d'avance, où une importante somme d'argent est promise en échange d'un paiement de mise en place.

Bonnes pratiques

Gérez bien votre mot de passe et vos questions secrètes

Effacez votre mémoire cache



Téléchargez la dernière version de votre fureteur Web

Sécurisez votre réseau sans fil

Suivez les règles de base pour transiger en toute sécurité

Conseils

- Activer l'authentification à deux facteurs pour les comptes importants
- Protégez les comptes importants en utilisant un mot de passe de trois mots aléatoires ou phrase-passe
- Créez un mot de passe distinct que vous utilisez uniquement pour votre compte de messagerie principal
- Mettez régulièrement à jour le logiciel et les applications sur vos appareils (idéalement mis à «mettre à jour automatiquement»)
- Enregistrez vos mots de passe dans un gestionnaire ou votre navigateur
- Pour vous protéger contre les rançons, sauvegardez les données importantes

Conseils pour repérer les signes révélateurs d'hameçonnage (phishing)

Repérer un courriel malveillant devient de plus en plus difficile, et de nombreuses escroqueries vont même tromper les experts en informatique.

Cependant, il y a quelques signes communs à surveiller:

- Autorité - L'expéditeur prétend-il provenir d'une personne officielle (comme votre banque, votre médecin, un avocat, un service gouvernemental)?

Les criminels prétendent souvent être des personnes ou des organisations importantes pour vous inciter à faire ce qu'ils veulent.

- Urgence - vous dit-on que vous avez un temps limité pour répondre (comme dans 24 heures ou immédiatement)?

Les criminels vous menacent souvent d'amendes ou d'autres conséquences négatives.

Suite des conseils …

- Émotion - Le message vous rend-il craintif, plein d'espoir ou curieux?

Les criminels utilisent souvent un langage menaçant, font de fausses demandes de soutien ou vous incitent à vouloir en savoir plus.

- Rareté - Le message offre-t-il quelque chose en nombre insuffisant (comme des billets de concert, de l'argent ou un remède pour des conditions médicales)?

La peur de manquer une bonne affaire ou une occasion peut vous faire réagir rapidement.

- Événements actuels - Vous attendez-vous à voir un message comme celui-ci? Les criminels exploitent souvent les actualités, les grands événements ou les périodes spécifiques de l'année (comme les déclarations fiscales) pour que leur arnaque vous paraisse plus pertinente.
- Votre banque (ou toute autre source officielle) ne devrait jamais vous demander de fournir des informations personnelles à partir d'un courriel.

Si vous avez des doutes sur un message, appelez-les directement.

N'utilisez pas les numéros / adresse courriel malveillante dans un courriel, mais visitez plutôt le site officiel.

Devenez une cible plus difficile

Les cybercriminels utilisent des informations publiques vous concernant pour rendre leurs messages malveillants plus convaincants.

Facilement disponibles sur les médias sociaux (tel que Facebook), d'où l'expression:

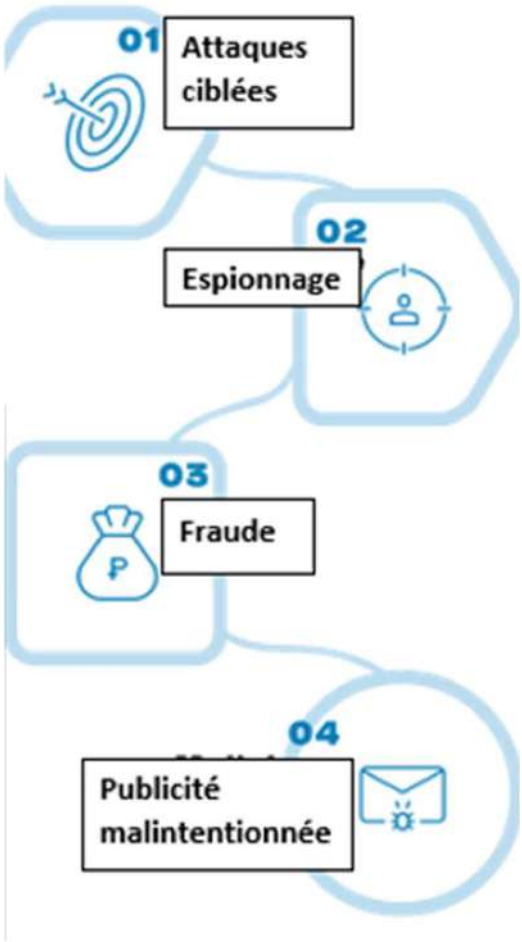
« empreinte numérique »

Vous pouvez vous rendre moins susceptible de recevoir des courriels malveillants en procédant comme suit

- Pour vos applications de médias sociaux et autres comptes en ligne, revoyez en modifiant vos paramètres de confidentialité.
- Pensez à ce que vous publiez sur Facebook par exemple et qui peut le voir: privé, publique
- Soyez conscient de ce que vos amis, votre famille et vos collègues disent de vous en ligne, car cela peut également révéler des informations qui peuvent être utilisées pour vous cibler.
- Si vous repérez un courriel suspect, signalez-le comme spam courrier indésirable/malveillant dans votre boîte de réception: « pourriel »

Dites à votre fournisseur de messagerie que vous l'avez identifié comme potentiellement dangereux.

Il est important de se rappeler les bases
de la sécurité numérique
et de rester à jour avec les dernières nouvelles
en matière de cybersécurité,
de mises à jour.
Soyez prudent et maintenez
les règles d'hygiène informatique et numérique.


01
Attaques ciblées
02
Espionnage
03
Fraude
04
Publicité malintentionnée

De faux sites Netflix et Disney+ se multiplient sur la toile.
Leur objectif : voler vos données personnelles,
y compris vos données bancaires,
en proposant …
des offres d'abonnement gratuit!


TraceTogether

Suivi des contacts COVID-19: l'équilibre délicat entre la confidentialité et les efforts de secours

L’entente de conception entre Apple et Google implique la création d'interfaces de programme d'application (API) qui aideraient les autorités de santé publique à concevoir des applications avec des capacités de suivi des contacts.
Ces applications seraient alors disponibles à la fois dans l'App Store d'Apple et dans la boutique Google Play.

Suite …

Les gouvernements du monde entier ont commencé à explorer l'utilisation des applications de recherche des contacts comme moyen clé pour suivre et réduire la propagation du coronavirus .

Le traçage des contacts est une méthode pour avertir les personnes lorsqu'elles ont été exposées à quelqu'un qui a contracté une maladie grave comme COVID-19 .

Cette méthode a déjà été utilisée pour mieux comprendre et limiter la propagation du VIH, de la méningite et d'autres maladies.

Il permet également aux gouvernements ou aux autorités sanitaires d'identifier les personnes qui pourraient avoir été en contact étroit avec un cas confirmé de COVID-19 infecté.

La police de Longueuil signale des plaintes pour fraude liée au COVID-19

Longueuil -- Sept plaintes pour fraude ont été déposées jusqu'à maintenant auprès de la police de Longueuil en lien avec la pandémie du COVID-19.

- de faux sites d'approvisionnement médical
- des autorisations frauduleuses de services d'urgence
- des demandes de soutien financier des services municipaux et des représentants
- et des offres de prêt aux familles dans le besoin au milieu de la crise

La police demande aux gens de s'assurer que les organisations qui s'approchent d'eux sont enregistrées, et que les établissements avec lesquels ils achètent en ligne, existent vraiment.
Ils demandent aussi aux gens d'être au courant d'offres *étrangement* généreuses.

« Les cybercriminels utilisent l'appétit élevé pour les informations liées à la COVID-19 comme *une opportunité de livrer des cyberattaques et de voler les informations d'identification des utilisateurs.*
Les individus et les organisations doivent rester très vigilants. »

Évitez de cliquer sur des liens dans des courriels non sollicités et méfiez-vous des pièces jointes, et ne rendez pas les réunions publiques et assurez-vous qu'elles sont protégées par des mots de passe pour empêcher le piratage de la visioconférence.

Préparé par:
Michel Cloutier
Présentation du:
2020 04 23