Méfiez vous des arnaques et de la désinformation sur les vaccins contre la COVID 19

La campagne de vaccination est une arme essentielle dans la lutte mondiale contre la pandémie, mais c'est aussi un sujet qui risque d'être exploité par les fraudeurs et les fournisseurs de fausses informations.

Le déploiement des vaccins COVID-19 ne cesse de s'accélérer, ce qui laisse espérer que nous pourrons voir la fin de la pandémie et revenir à une vie normale plus tôt que tard. Cela n'a toutefois pas échappé aux escrocs entreprenants qui voudraient tirer profit de l'effort de distribution des vaccins en déployant des arnaques et en envoyant des e-mails frauduleux. Examinons quelques-unes des campagnes où les cybercriminels tentent de soustraire des informations personnelles et de l'argent à des citoyens numériques sans méfiance ou de diffuser des affirmations sans fondement sur les vaccins.

Offres commerciales frauduleuses

Une tactique courante consiste à proposer différentes façons de tirer parti de la pandémie et du déploiement des vaccins. Ces escroqueries portent généralement sur les vaccins COVID-19 eux-mêmes ou sur la technologie utilisée pour les fabriquer ou les stocker.

Dans le premier exemple ci-dessous, le cybercriminel se fait passer pour un employé d'une société pharmaceutique, ce qui implique qu'il est d'une manière ou d'une autre impliqué dans les efforts de fabrication des vaccins. Afin d'instaurer un certain degré de confiance, l'escroc en puissance laisse tomber le nom de Whitman Laboratories, une véritable société pharmaceutique britannique qui n'est pas impliquée dans un tel comportement scélérat. En outre, cet escroc opte pour un fournisseur de courrier électronique chiffré, au lieu des habituels favoris des fraudeurs comme Gmail ou Hotmail


CVD-19 Vaccine Business Proposal

Hello,

I am Elliot Grayson Research Assistant at Whitman Laboratories Ltd UK. One of the leading Bio Pharmaceutical companies in Europe. I have a business proposal concerning COVID-19 Vaccine for you which is worth a substantial amount and will save lives. I would be glad to receive your acknowledgement of this email so I can furnish you more with details of my proposal for your consideration. Please send your reply to my private email at: @protonmail.com

Please give me the opportunity to explain to you in detail what the business is all about by replying back to my private email as stated above. Note: You have the right to quit by the end of my detailed explanation and you don't feel like moving forward with me. But trust me, you won't regret it.

Elliot Grayson,
Whitman Laboratories Ltd.

Au-delà de ces deux points, le reste du courrier électronique porte toutes les marques d'une escroquerie – il est peu détaillé, probablement pour susciter une réponse, et comporte des erreurs de grammaire et des choix stylistiques bizarres. Il convient également de noter que presque toutes les négociations relatives à la vente du vaccin COVID-19 se font directement entre les fabricants et les gouvernements, de sorte qu'un assistant de recherche qui appelle à froid des acheteurs potentiels devrait à tout le moins soulever des doutes.
En revanche, le deuxième exemple pourrait être considéré comme étant l'opposé du premier. Le fraudeur derrière cet e-mail prétend vendre des unités de congélation de qualité laboratoire, dont certains vaccins ont effectivement besoin pour ne pas commencer à se

dégrader. Dans ce cas, les escrocs ont fait leurs devoirs et ont tout fait pour que l'e-mail semble aussi plausible que possible, allant même jusqu'à ajouter un peu de marketing. D'une part, le fabricant existe, il possède presque tous les certificats revendiqués dans le courrier électronique et, en fait, il fabrique les congélateurs annoncés en différentes tailles.

Par ailleurs, plusieurs caractéristiques classiques des arnaques par e-mail sont clairement visibles : l'objet du message est bizarre et comporte des fautes d'orthographe dans le nom de l'entreprise, le message de salutation est général, impersonnel et communément rencontré dans d'autres domaines familiers de l'escroquerie par courrier électronique. De plus, le message est truffé de fautes de grammaire et ne comporte pas de signature. En outre, le produit proposé se concentre sur un marché de niche : on trouve rarement ce type de congélateurs dans un cabinet médical ou même dans la plupart des hôpitaux ou des pharmacies.

Les faux paiements liés à la COVID-19

Une autre tactique fréquemment utilisée par les arnaqueurs consiste à se faire passer pour une autorité sanitaire directement impliquée dans la lutte contre la pandémie. L'Organisation mondiale de la santé (OMS) a été l'une des autorités les plus personnifiées dans diverses campagnes d'escroquerie liées à COVID-19, les escrocs – se faisant passer pour des représentants et des employés de l'OMS – essayant de diffuser de fausses applications ou prétendant fournir des informations importantes.

L'OMS n'est en aucun cas la seule autorité dont l'identité est usurpée par ces cybercriminels. Dans l'exemple suivant, les escrocs se font passer pour les Centres américains de contrôle et de prévention des maladies (CDC). Ici, les fraudeurs obtiennent en fait certaines informations exactes – le CDC dispose en effet d'un centre d'opérations d'urgence et de programmes qui travaillent en tandem avec des partenaires de santé publique. Toutefois, si l'on examine le courrier électronique de plus près, les signes d'une escroquerie sont plus qu'évidents. Si vous êtes l'un des partenaires du CDC, vous connaissez probablement sa mission et n'avez pas besoin d'un rappel, et à moins d'avoir passé les derniers mois dans une grotte, vous savez certainement déjà que plusieurs vaccins ont été développés, testés et que certains ont déjà été approuvés.

Qui plus est, le formatage de l'e-mail est brouillon et confus, le message est truffé de fautes

de frappe et de structures de phrases bizarres, et surtout il ne précise pas pourquoi le partenaire devrait recevoir ce gros paiement. Une autre chose qui ressort est le nom de la personne réputée responsable du paiement. Si David W. Archey est un véritable agent qui travaille pour le Federal Bureau of Investigation (FBI), il n'y a aucune raison pour qu'il soit la personne chargée de livrer les paiements d'une autre agence fédérale.

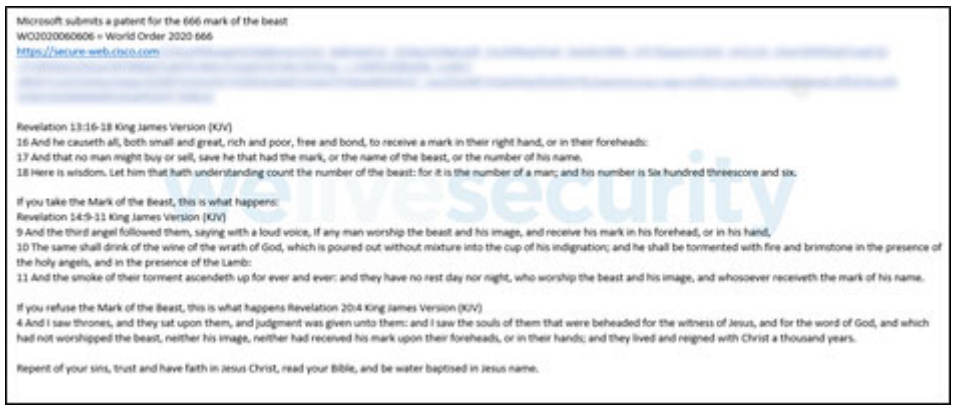
Des théories conspirationnistes à foison

Même si nous voudrions nier l'existence des théories du complot et des canulars, l'internet en regorge aujourd'hui. Si vous cherchez bien, vous trouverez probablement des mensonges viraux pour à peu près n'importe quel sujet. En ce moment, les fausses informations concernant les vaccins contre la COVID-19 sont au premier plan

Ces intox sont également l'occasion de propager d'innombrables e-mails contenant une foule de liens qui prétendent révéler la « vérité », ce qui consiste généralement à prendre une nouvelle ou une vidéo et à l'embellir pour l'adapter à leur récit. Une autre tactique courante consiste à prendre ce qui est dit et à le déformer, à le citer de manière erronée ou à le cadrer de telle sorte que le résultat final ne ressemble à rien par rapport à l'original. Tout cela est fait dans le but de produire une valeur de choc et de convaincre les gens de cliquer sur les liens.
L'un de ces courriers électroniques non sollicités utilise une véritable interview de Bill Gates qui est modifiée de manière trompeuse afin de déformer son point de vue. Il diffuse également diverses faussetés qui s'appuient sur des affirmations sans fondement provenant de diverses sources afin de « prouver » son point de vue, notamment des vidéos qui répandent des croyances erronées sur les vaccins. Ces vidéos sont disponibles à la fois sur YouTube et sur un site d'hébergement de vidéos particulièrement populaire auprès des extrémistes et des fournisseurs de fausses histoires.

Pour couronner le tout, l'e-mail fait également référence à de véritables composés chimiques et à des brevets qui sont également librement consultables sur Internet. Encore une fois, ces références sont utilisées parce qu'elles s'intègrent parfaitement dans le récit et devraient susciter la curiosité au point d'inciter les lecteurs à cliquer sur le lien.

Un autre e-mail du même acabit traite d'un nouveau brevet déposé par Microsoft. Tout cet e-mail est construit autour du nombre de la bête, qui coïncide avec le numéro de publication du brevet. Mais rassurez-vous ; une recherche rapide sur le portail de la propriété intellectuelle de l'Organisation mondiale de la propriété intellectuelle (OMPI) révèle que ce que le géant technologique de Redmond a breveté n'est qu'un système de cryptomonnaie qui utilise des données sur l'activité corporelle. Aucun de ces e-mails n'est malveillant, mais ils peuvent être classés comme propageant de la désinformation en ligne. Ainsi, vous n'avez pas à vous inquiéter des prédictions de l'apocalypse pour l'instant.



Ce n’est pas ce que le médecin a dit!

Ce ne sont là que quelques exemples d’escroqueries liées aux vaccins sur lesquels vous pourriez tomber et vous pouvez être sûr que des escrocs entreprenants redoubleront d’efforts à mesure que le déploiement du vaccin se poursuivra. En outre, étant donné l’augmentation rapide des nouvelles variantes de coronavirus, il ne serait pas surprenant de voir ces cas apparaître dans les escroqueries liées à la pandémie de COVID-19. L’un des moyens les plus simples de se protéger consiste à utiliser une solution de sécurité réputée qui comprend un filtre anti-spam. Toutefois, si vous recevez un e-mail non sollicité d’une personne que vous ne connaissez pas : soyez toujours très vigilant et examinez-le à la recherche de signes révélateurs d’une escroquerie, y compris ceux décrits ci-dessus.

En outre, voici quelques conseils qui vous aideront à vous protéger contre diverses tentatives d’escroquerie :

- Évitez de cliquer sur des liens ou de télécharger des fichiers que vous avez reçus par courrier électronique d’une source que vous ne connaissez pas et que vous ne pouvez pas vérifier de manière indépendante
- Si vous avez reçu un e-mail censé provenir d’une organisation officielle, consultez son site web officiel et contactez-les en utilisant leurs coordonnées officielles pour déterminer s’ils vous l’ont vraiment envoyé
- Soyez prudents face aux offres commerciales qui semblent trop belles pour être vraies ou aux offres d’expéditeurs non vérifiés
- Utilisez une solution de sécurité multicouche réputée qui comprend une protection contre le spam, les tentatives d’hameçonnage et d’autres menaces.

Cette lettre d’information a pour objectif d’informer sur l’actualité de nos marques et du marché qui les entoure. Afin de vous proposer un service au plus près de vos attentes, n’hésitez pas à nous faire part de vos remarques et suggestions :

JE DONNE MON AVIS