Attention à ces fraudes populaires sur WhatsApp

WhatsApp est populaire, et pour cause ; vu que cette application vous permet de communiquer à travers des réseaux sans fil, gratuitement et avec des personnes situées dans le monde entier : des avantages que les services de messagerie traditionnels, fournis par les opérateurs de téléphonie mobile, ne sont pas en mesure de vous proposer. Malheureusement, la popularité de cette application attire également de nombreux escrocs. La variété des fraudes est considérable, raison pour laquelle les utilisateurs de WhatsApp se voient exposés à pas mal de risques, où qu'ils se trouvent. Apprenez-en plus sur certaines fraudes populaires sur WhatsApp et la manière de vous en protéger.

Versions falsifiées de WhatsApp

Pour toujours posséder la bonne version de WhatsApp, veillez à ne jamais télécharger et installer l'application à partir d'un lien que l'on vous a envoyé. Il convient de ne télécharger des applications que depuis l'app store officiel, qui varie selon la plate-forme de votre dispositif (Google Play, App Store d'Apple, etc.). Si vous doutez de la version installée sur votre appareil, veuillez supprimer l'application puis la télécharger à nouveau depuis l'app store officiel.

Messages vocaux falsifiés

Source: www.business2community.com

Cette fraude n'est rien d'autre qu'un message vocal falsifié : il suffit de cliquer sur le lien fourni pour tomber dans le piège !

Vous recevez un message avec pour objet « Incoming Voice Message ». Il vous suffit de cliquer sur le lien pour permettre aux pirates informatiques d'accéder à vos informations personnelles et même de bloquer l'accès à votre appareil !

WhatsApp Gold

WhatsApp Gold est une escroquerie propagée à travers les réseaux sociaux. Il s'agit d'une version premium falsifiée, associée en partie à un statut d'élite et offrant des fonctionnalités spéciales qui, apparemment, ne sont pas disponibles sur le programme initial.

Une fois que vous vous abonnez à cette mise à jour falsifiée, vous devez payer un montant mensuel atteignant jusqu'à 40 dollars par mois. Une version actualisée de cette fraude, nommée « WhatsApp Elegant Gold », circule entre-temps sur Internet. Celle-ci mène les utilisateurs à une page web vous invitant à saisir votre numéro de téléphone, en vue de recevoir une nouvelle édition « améliorée » de WhatsApp.

Espionnage par WhatsApp

Source : gizmostorm.com

Il existe, en réalité, différentes applications permettant d'espionner d'autres personnes à travers WhatsApp. Malheureusement, si vous lancez la recherche « WhatsApp espionnage », vous trouverez même davantage d'articles vous expliquant comment espionner que d'articles illustrant comment s'en protéger.
Cependant, il y a un hic : la majorité de ces applications d'espionnage sont en vérité des fraudes déchargeant des malwares sur votre appareil. Par conséquent, si vous êtes tenté de vous en servir, ayez conscience de ce que vous êtes susceptible d'attraper !

Hameçonnage par WhatsApp chez Migros

Un sondage, prétendument réalisé par Migros, se répand actuellement comme une traînée de poudre sur WhatsApp. Ce sondage promet un bon d'achat d'une valeur de 500 francs en guise de récompense.

Il existe des arnaques du même type pour McDonald's, IKEA, H&M, KFC, Zara, ainsi que d'autres grandes entreprises. Ces fraudes sont traduites dans plusieurs langues, ce qui augmente encore le nombre de victimes potentielles dans le monde entier ; elles visent à s'emparer de vos informations personnelles en vous donnant de faux espoirs.

Envoi de messages surtaxés

WhatsApp offre aux cybercriminels une nouvelle façon de se livrer à des comportements malveillants ; L'envoi de SMS surtaxés malveillants a été récemment déterminé par le Laboratoire de F-Secure comme la menace mobile ayant la plus forte croissance. Fondamentalement, les utilisateurs reçoivent un message qui leur demande une réponse : « Je vous écris de WhatsApp, dites-moi si vous avez reçu mes messages », « Contactez-moi au sujet du second entretien d'embauche », ou d'autres messages à caractère sexuel, entre autres. Lorsque vous répondez à ces messages, vous êtes automatiquement redirigé vers un service surtaxé.

Comment reconnaître une fraude par WhatsApp

Les fraudes par WhatsApp ont connu un essor, mais vous ne devriez pas renoncer pour autant à vous servir de cette application utile et amusante. WhatsApp permet à tout le monde de communiquer avec le reste de la planète, et cela gratuitement. Pour empêcher de vous faire avoir par des escrocs, veuillez garder à l'esprit les tuyaux suivants :
s'agit probablement d'une fraude. Comme WhatsApp l'indique sur son propre site internet, « nous n'utilisons jamais de WhatsApp pour vous envoyer des messages. »

1. Soyez sceptique face à tout message de WhatsApp

Tout message provenant directement de WhatsApp, reçu à travers l'application, devrait vous mettre immédiatement la puce à l'oreille. WhatsApp ne ferait jamais cela ; si vous recevez un message convaincant, directement de l'entreprise elle-même, rappelez-vous qu'il s'agit probablement d'une fraude. Comme WhatsApp l'indique sur son propre site internet, « nous n'utilisons jamais de WhatsApp pour vous envoyer des messages. »

2. Attention aux messages sollicitant vos informations personnelles

En général, WhatsApp (ou toute autre application légitime) ne vous demandera jamais de fournir vos informations personnelles de façon aléatoire. Si vous doutez de la légitimité d'une demande, vous pouvez, à tout moment, consulter le site web de WhatsApp et envoyer un mail au service-clientèle. Si votre application de messagerie ne vous fournit pas de coordonnées pour le service-clientèle, veuillez contacter d'autres utilisateurs pour savoir s'ils ont remarqué des incidents suspects.

3. Vous n'avez probablement pas gagné

À moins que vous n'ayez participé directement à un concours, il s'agira probablement d'une fraude. Il serait tentant de vous croire gagnant, mais comment gagner 500 € sans avoir rien fait ? Sans même avoir complété un sondage. Vous savez ce que l'on dit : si cela semble trop beau pour être vrai, c'est que ce n'est probablement pas vrai.

4. Ne partagez jamais votre adresse MAC ou IMEI

Tout dispositif mobile dispose d'un numéro IMEI (International Mobile Equipment Identity) ou d'une adresse MAC (media access control) permettant de l'identifier. Votre compte WhatsApp est directement lié à votre téléphone par le biais de ce numéro spécial, qui équivaut donc à un mot de passe pour votre compte. Une fois qu'un pirate informatique est parvenu à obtenir votre numéro de téléphone et votre adresse MAC ou IMEI, il sera facile pour lui d'accéder à votre compte.

N'oubliez pas : même les personnes les plus prudentes peuvent se faire avoir dans un moment de négligence. Équipez votre appareil d'une solution anti-malware et renseignez-vous sur le mode de communication utilisé par votre application de messagerie avec ses utilisateurs. Vous pouvez bel et bien vous servir des applications les plus récentes et merveilleuses, mais préparez-vous pour le pire des cas : après tout, prudence est mère de sûreté.

Si vous souhaitez en savoir plus sur des fraudes plus anciennes via WhatsApp et sur la manière de vous en protéger, nous vous invitons à lire d'autres articles relatifs à WhatsApp publiés sur notre blog.

Nous vous souhaitons une bonne navigation (sans fraude) !