WHATSAPP - LE FISHING DANGEREUX !

Categories: À la une !, Actualités ADC FRANCE, Internet et box, Justice, police, Les conseils
Tags: Actualités, Conseils, Scandale



> ## *HAMEÇONNAGE AUX FAUX VOTES POUR DES CONCOURS SUR WHATSAPP*

Le site cybermalveillance.gouv.fr a publié une alerte importante sur du fishing particulièrement dangereux pour les titulaires de comptes whatsapp !

Le texte intégral est consultable avec le lien ci-dessous :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/vigilance-faux-vote-whatsapp

Nous publions des extraits de ce communiqué :

De quoi s'agit-il ?

La victime reçoit un message, le plus souvent sur WhatsApp, provenant en apparence d'un de ses contacts.

Ce message l'invite à soutenir une personne dans un vote en ligne lié à un concours – souvent de ballerines – ou à une bourse d'études.

Le lien contenu dans ce message redirige vers une fausse page de vote, créée pour ce prétendu concours.

La victime est ensuite incitée à saisir son numéro de téléphone, associé à son compte WhatsApp, sous prétexte de valider son vote.

En réalité, cette étape permet de générer un code qui autorise l'ajout d'un nouvel appareil au compte WhatsApp de la victime, au profit de l'escroc.

La victime est ensuite amenée à saisir elle-même ce code dans les paramètres de son compte, selon les instructions affichées sur la page frauduleuse.

Le cybercriminel détourne ainsi la fonctionnalité d'ajout d'un nouvel appareil de WhatsApp afin de prendre le contrôle du compte de la victime.

NDLR : Le gras / rouge a été ajouté par nos soins.

Il est publié quelques messages :

Exemples de textes de messages frauduleux

Coucou ! Sophie, la fille de mes amis est dans un concours pour une bourse d'études et l'occasion de monter sur scène. Un vote pour elle ? Merci !

Salut, pourrais-tu voter pour Eliska ? C'est la fille de mes amis. Le premier prix est un cours de danse gratuit et c'est très important pour elle!

Quelles sont les conséquences pour les victimes ?

- ***Compromission du compte WhatsApp et usurpation d'identité**, permettant la rediffusion de l'arnaque auprès des contacts enregistrés ;*
- ***Utilisation frauduleuse du compte à des fins d'escroqueries financières** : demande d'argent à des proches, arnaque au proche en situation d'urgence… ;*
- ***Chantage** lié à l'accès à des **données personnelles** présentes sur le compte (**photos, vidéos, échanges sensibles**, etc.) ;*
- ***Perte d'accès au compte WhatsApp**, l'escroc pouvant ensuite en bloquer l'usage à la victime, voire exiger une rançon pour le restituer.*

NDLR : Le gras a été mis par le site cybermalveillance.gouv.fr. Le rouge a été ajouté par nous.

Nos recommandations :

Pour les personnes ayant été victimes :

- ***Vérifier sans délai la liste des appareils connectés dans les paramètres du compte et supprimer tout appareil inconnu*** *;*
- ***Avertir ses contacts de la compromission du compte et de l'existence de l'arnaque*** *;*
- ***Contrôler les paramètres du compte afin d'identifier d'éventuelles modifications, notamment les coordonnées associées*** *: numéro de téléphone, adresse électronique de récupération, vérification en deux étapes, mot de passe, liaison à un compte Instagram et/ou Facebook, etc. ;*
- ***Si l'accès au compte est perdu : suivre la procédure officielle de WhatsApp*** *: ;*
- *Consulter également notre article dédié au piratage de compte.*

Pour les personnes ayant reçu ce message sans être victimes :

- ***Informer le contact concerné que son compte semble compromis****, de préférence par un autre moyen que WhatsApp, car il pourrait ne pas voir le message.*

NDLR : Le gras a été mis par le site cybermalveillance.gouv.fr

En conclusion dés lors qu'une demande sort d'un cadre ordinaire, tout doit être vérifié !!!