ARNAQUES ET SPAMS À ÉVITER SUR FACEBOOK

« LIKE- » OU « SHARE-BAITING»
(INCITER LES UTILISATEURS À CLIQUER SUR LES BOUTONS « J'AIME » OU « PARTAGER »)

1. Les escrocs vous incitent à cliquer sur le bouton «J'aime » ou « Partager » d'une page Facebook en vous promettant des privilèges ou un accès à du contenu inaccessible à partir de Facebook ou d'un autre site
2. Après avoir cliqué sur « J'aime », vous êtes redirigés vers une enquête vous invitant à fournir des informations personnelles. Chaque vue de la page rapporte une commission à son auteur !

CONSEILS

Facebook a intégré à ses boutons « J'aime » une protection contre le clickjacking (ou détournement de clic). Ainsi, il peut vous être demandé de confirmer votre « J'aime » lorsque vous visitez un site jugé suspect, et ce afin d'éviter toute attaque

« CLICKJACKING » (DETOURNEMENT DU CLIC) DU BOUTON « J'AIME »

1. Des pages malveillantes contiennent des boutons «J'aime » cachés. On vous propose une vidéo intéressante avec son bouton de lecture. En cliquant sur ce bouton, la vidéo ne se lance pas : vous cliquez en réalité sur le bouton « J'aime » qu'il dissimule.
2. Certaines pages vous invitent même à cliquer plusieurs fois, chaque clic générant plusieurs «J'aime ».

CONSEILS

Méfiez-vous des liens qui promettent du contenu sensationnel et incitent les utilisateurs à cliquer plusieurs fois sur des parties spécifiques de l'image.

APPLICATION MALVEILLANTE

1. Il peut arriver que vous installiez une application Facebook qui s'avère malveillante. L'application prend alors possession de votre page, donnant au cybercriminel la possibilité de publier sur votre mur, d'accéder à vos messages et de chatter avec vos amis.
2. Il s'agit de l'un des arnaques les plus anciennes et les plus répandues sur les réseaux sociaux, alors prenez garde !

CONSEILS

Lorsque vous installez des applications, soyez prudents et regardez de très près les autorisations requises par l'application. En cas de doute, ne l'installez pas !

ATTAQUES PAR COPIER-COLLER

1. On vous propose d'accéder à une vidéo ou à un site Web intéressant, en effectuant un copier-coller du site Web dans la barre d'adresse de votre navigateur.
2. Un code auto-exécutable dépose alors un spam à votre nom. Néanmoins, vous conservez le contrôle du compte.

CONSEILS

Ne collez jamais une adresse de site Web ou du texte inconnus dans la barre d'adresse de votre navigateur.

HOAX (CANULARS)

1. Avez-vous déjà vu une histoire sensationnelle ou découvert une mise à jour de statut choquante dans votre fil d'actualités ? Attention ! Il s'agit généralement de hoax (canulars) créés pour circuler sur Facebook.
2. L'objectif des canulars est soit de générer du trafic sur un site de spam, soit simplement de piéger les autres utilisateurs.
www.facebook.com/hacked

CONSEILS

Résistez à la tentation de publier des messages non vérifiés qui encouragent vos amis à les publier à leur tour.

NETTOYAGE DE VOTRE COMPTE

Supprimez les publications offensantes
Si des arnaques ont été publiées sur votre mur, vous pouvez les supprimer comme n'importe quelle autre publication que vous souhaitez supprimer, en cliquant sur la croix « x » accompagnant la publication.

Supprimez les applications suspectes
Si vous avez accidentellement installé une application malveillante ou si vous pensez l'avoir fait, vous pouvez gérer et supprimer n'importe quelle application à partir de votre profil de compte.

Changez votre mot de passe
Les utilisateurs peuvent se rendre sur www.facebook.com/hacked afin de sécuriser leur compte s'ils pensent qu'il a été piraté.