Arnaque Le Bon Coin : vague de phishing par SMS

Les SMS sont de plus en plus utilisés pour correspondre avec une entreprise ou bien entre acheteur et vendeur, et les cyber-escrocs en profitent.

Que vous soyez un habitué ou non de la célèbre plateforme de vente et d'achat de biens d'occasion, nous vous recommandons de lire avec attention ce qui est arrivé à plusieurs utilisateurs et utilisatrices et qui pourrait malheureusement arriver à d'autres entreprises à travers le monde.

Il est aujourd'hui fréquent d'afficher son numéro de téléphone dans une annonce afin d'espérer trouver rapidement un acheteur. Cependant, des cyber-escrocs y ont vu une opportunité pour voler des informations personnelles.

Comment fonctionne l'arnaque par phishing sur LeBonCoin ?

Pour commencer, la personne reçoit un SMS indiquant qu'un prépaiment a été fait et contenant un lien web. Elle clique dessus et arrive alors sur une page web ressemblant comme deux gouttes d'eau au site officiel Le Bon Coin. La texte contient pourtant quelques fautes d'orthographe et l'adresse web du site est "od-leboncoin.info" au lieu de www.leboncoin.fr.

Ensuite, l'utilisateur est invité à télécharger la soi-disant dernière version du site suite à une notification affichée sur la page. Elle clique alors sur "continuer" puis doit "confirmer une commande" sous peine d'annulation, bien qu'il n'y ait eu aucune commande faite de la part de la victime.

Qu'espèrent obtenir les cyber-escrocs ?

Bien que le site de phishing affirme que le paiement de la commande en question a été reçu, les références du compte de la victime sont bien entendu erronées. La personne devra pourtant vérifier l'exactitude des coordonnées bancaires via un paiement d'un montant de 0,01 €. C'est à ce moment là que les cyber-escrocs obtiendront les coordonnées bancaires de leur victime.

La somme peut sembler faible et dissuader un grande nombre de personnes averties, mais sachez que 18,5 millions de Français ont vendu ou bien acheté via le Bon Coin en 2018, ce qui laisse beaucoup de chance aux arnarqueurs de trouver une proie.

Que faire ?

Le service client du site web Le Bon Coin a alerté ses clients et rappelle que ces messages visent à récupérer les données personnelles des victimes et qu'aucun SMS ne sont envoyés à ses utilisateurs.

Rester vigilants et porter attention aux fautes d'orthographe et aux adresse web affichées dans le corps du texte et dans votre navigateur.

Signaler tous messages douteux via le site www.33700.fr, plateforme officielle de lutte contre les SMS indésirables.

Si vous souhaitez utiliser le service de paiement sécurisé mis en place par la plateforme en 2018, passez directement par le système de messagerie du site internet. Le vendeur doit, au préalable, renseigner son IBAN depuis son compte LeBonCoin, afin de recevoir l'argent par le biais du service de paiement sécurisé.

Nous vous recommandons également de ne pas cliquer sur les liens contenus dans ce type de SMS. Répondre à un message de sollicitation, même pour manifester son désintérêt, prouve au cyber-escroc que l'adresse e-mail ou le numéro de téléphone sont actifs. Les tentatives de phishing ou de spam ne feront que continuer

Les cyber-escrocs n'attendent pas toujours que vous regardiez votre boîte email pour essayer de voler vos données personnelles au travers d'un lien qui vous mènera vers un faux site web. Ils envoient également des sms - d'où le nom smishing - pour vous prévenir d'un soi-disant problème important à régler avec une URL (adresse web) raccourcie pour ne pas éviter les soupçons.

Vous cliquez alors malheureusement dessus en pensant qu'il s'agit d'un message tout à fait légitime et arrivez sans le savoir sur un site web ressemblant comme deux gouttes d'eaux à celui du portail Free mobile. Est-il trop tard ?