Ecrit par Echo du Mardi le 1 février 2023

Les 11 arnaques aux applications de paiement à connaître

Qu'il s'agisse de partager l'addition après une soirée ou d'envoyer de l'argent pour un cadeau, nous sommes de plus en plus nombreux à faire confiance aux applications de paiement comme Lydia, Cash App ou encore PayPal. C'est un moyen rapide et transparent d'effectuer des transactions financières. Les deux principales fonctions de ces applications étant de payer les autres et d'être payé. Deux actions particulièrement sensibles aux cyberattaques. Elles offrent ainsi quelques dispositifs de sécurité particuliers pour vous protéger comme le chiffrement, les verrous de sécurités, les notifications ou encore les désactivations de paiement à distance. Mais malheureusement, cela ne suffit pas vous pourriez subir l'une de ces 11 arnaques courantes :

· **Un faux service d'assistance :** Les escrocs des applications de paiement profitent souvent des

Ecrit par Echo du Mardi le 1 février 2023

utilisateurs en se faisant passer pour le service d'assistance. Or, ces services d'assistances ne vous demanderont jamais de fournir votre code d'accès ou votre code PIN, d'envoyer un paiement, de faire un achat, de télécharger une application pour un « accès à distance », ou d'effectuer une transaction « test » de quelque nature que ce soit. Si vous recevez un message qui semble provenir du support d'une application aller directement dans l'application pour le contacter, sans répondre au message.

· **Des offres alléchantes :** L'une des arnaques les plus populaires est celle des escrocs qui proposent des biens ou des services coûteux – mais fictifs – en échange d'un paiement. Les paiements d'applications sont instantanés et ne peuvent généralement pas être annulés. N'oubliez pas que si quelque chose semble trop beau pour être vrai, il s'agit probablement d'une escroquerie.

· **Des dépôts aléatoires :** Un dépôt d'argent aléatoire est souvent utilisé pour endormir les utilisateurs et leur donner un sentiment de confiance envers les escrocs. Cependant, les escrocs peuvent vous envoyer un paiement « par accident » et vous demander de leur renvoyer le montant du paiement. Le montant que vous leur renvoyez provient des fonds de votre compte. Ces escrocs contestent le paiement auprès de leur banque ou de leur carte de crédit après que vous avez renvoyé les fonds. Cela signifie qu'ils seront remboursés à la fois par vous et par leur banque.

· **Un gain fictif :** Vous pouvez être contacté pour réclamer de fabuleux prix en espèces. Mais pour recevoir le prix, ils doivent d'abord envoyer de l'argent. Les applications de paiement ne demandent pas à leurs utilisateurs de payer pour les concours ou les promotions, donc les demandes d'envoi d'argent pour réclamer un prix sont probablement frauduleuses.

· **Une demande de numéro de sécurité sociale :** En général, il est préférable de ne communiquer votre numéro de sécurité sociale qu'à des sources de confiance et vous devriez éviter de communiquer des informations d'identité importantes aux demandeurs sur n'importe quelle application.

· **Des aides gouvernementales :** Certains escrocs peuvent promettre de l'argent sous la forme d'une subvention gouvernementale ou d'un programme d'aide. Mais toute demande d'informations financières est un signe révélateur d'une escroquerie.

· **Les « cash flippers » :** Les escrocs peuvent prétendre être en mesure de « retourner » les fonds des utilisateurs afin de gagner plus d'argent. L'escroquerie au cash flipping est conçue pour prendre l'argent des utilisateurs sans jamais leur donner de retour sur investissement.

· **De faux remboursements :** Si vous vendez quelque chose sur un marché en ligne, un escroc peut vous contacter en prétendant qu'il est intéressé par l'article et qu'il effectuera un paiement via une applications de paiement – sauf que vous ne recevrez pas l'argent et qu'il prétendra avoir envoyé le paiement plusieurs fois. Il exigera le remboursement de votre propre argent pour un article qu'il n'a jamais payé.

· **Une fausse histoire d'amour :** Si vous rencontrez quelqu'un sur une application de rencontre ou un réseau social et qu'il vous demande de lui envoyer de l'argent via une application de paiement, soyez extrêmement prudent. Si une personne que vous n'avez pas rencontrée en personne prétend avoir des

Ecrit par Echo du Mardi le 1 février 2023

intentions romantiques et vous demande de l'argent, soyez méfiant.

· **Un e-mail de phishing :** Les équipes de l'application ne vous demanderont jamais de fournir des informations de connexion ou n'utiliseront pas un langage menaçant dans leurs messages. Si vous recevez ce qui semble être un e-mail de phishing, vous devez contacter le support via l'application.

· **De fausses alertes de sécurité :** Certains escrocs peuvent envoyer un e-mail frauduleux prétendant que votre compte a été compromis et que vos informations personnelles ont été divulguées. Les escrocs incluent souvent des liens vers de faux sites Web dans les e-mails qui vous invitent à modifier vos identifiants de connexion, mais cette astuce peut en fait voler vos informations de connexion existantes.

Vous l'aurez compris il existe de nombreuses manière d'accéder à vos données via les applications de paiement, assurez-vous d'en être conscient et d'avoir les bons réflexes.

Bastien Bobe, directeur technique Europe continentale chez Lookout