UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

LES MULTIPLES FORMES D'HAMEÇONNAGE

Lorsque l'hameçonnage est évoqué, la première pensée des utilisateurs se tourne souvent vers les courriels malveillants qui inondent leurs boîtes de réception. Cependant, il est crucial de comprendre qu'il se présente sous diverses formes, et chacune de ces manifestations représente une menace sérieuse à ne pas sous-estimer. Ces menaces peuvent mettre en péril la sécurité des données, qu'elles soient personnelles ou professionnelles, ainsi que celles de nos éventuels contacts. Les acteurs malveillants utilisent désormais des stratégies variées pour piéger les utilisateurs, privilégiant notamment des méthodes d'ingénierie sociale pour inciter leurs cibles à divulguer des informations sensibles.

LE RISQUE DANS LES RÉSEAUX SOCIAUX

Malgré les mesures prises par les fournisseurs de services de réseaux sociaux pour prévenir les messages d'hameçonnage, il peut encore arriver de recevoir des messages incitant à cliquer sur des liens ou à télécharger des fichiers. Ce qui est particulièrement inquiétant, c'est que ces messages peuvent parfois sembler provenir de contacts déjà présents dans la liste d'amis, leur propre compte ayant été compromis. Dans de telles situations, les réflexes peuvent inciter à accorder confiance au contenu envoyé, sans se rendre compte qu'il provient en réalité d'un attaquant.

LE RISQUE DANS LES PLATEFORMES DE COLLABORATION

Récemment, il est devenu plus fréquent de constater des tentatives d'hameçonnage sur les plateformes de collaboration professionnelles telles que Microsoft Teams. Des individus qui ne font pas partie de l'organisation envoient des messages qui donnent l'impression d'être un participant au projet en cours. Ils incitent les utilisateurs à consulter de la documentation ou à cliquer sur des liens vers des sites Web, déclenchant involontairement l'exécution d'un logiciel malveillant qui compromet le compte ou les informations de l'utilisateur. Cela donne ensuite à un acteur malveillant le contrôle sur le compte, lui permettant ainsi de continuer à envoyer des messages d'hameçonnage en utilisant l'identité de la victime.

COMMENT SE PROTÉGER

Toujours se méfier des liens et des fichiers. Il est important de ne jamais avoir une confiance aveugle sur les liens et fichiers qui nous sont transmis, surtout lorsque ceux-ci nous redirigent vers des ressources externes et inconnues.

Il est important de toujours valider l'identité d'une personne qui nous demande de l'information sensible. Contacter la personne par voix ou vidéo, ou par le biais d'une autre plateforme afin de vérifier qu'elle est bien la personne avec qui vous parlez.

Toujours se méfier des messages inattendus. Il est important d'avoir une vigilance accrue lorsqu'on reçoit un message contenant un lien ou un fichier, surtout lorsque ce message n'est pas attendu.

Il est important de toujours se méfier des demandes d'amis inconnus. Un étranger pourrait vouloir s'ajouter à votre réseau d'amis afin d'espionner vos publications, espérant y retirer de l'information pouvant être utile à la déduction de vos mots de passe ou vos questions de sécurité.