03.03.2022

Comment faire perdre la tête aux arnaqueurs

Les cybercriminels trouvent toujours de nouvelles méthodes pour vider les comptes bancaires de leurs victimes. Justement, une vidéo a attiré notre attention dans la mesure où elle traite d'un danger très actuel avec beaucoup d'humour.

Au-delà de son côté divertissant, la vidéo (en suisse allemand) aborde une méthode très utilisée actuellement par les cybercriminels. Jugez-en par vous-même : www.youtube.com/watch?v=8_5eQw-kdyM (http://www.youtube.com/watch?v=8_5eQw-kdyM)

Le danger évoqué dans le film, à savoir la saisie automatique de l'adresse de l'institut bancaire dans la fenêtre de recherche Google, peut être évité grâce aux mesures suivantes :

- Tapez toujours manuellement l'adresse de votre institut financier, directement dans la barre d'adresse du navigateur, et non dans la fenêtre de recherche de Google !
- Ne tapez jamais « Login maBanque » ou « E-Banking maBanque » ou tout autre formule similaire dans la fenêtre de recherche Google. Avant de lister les résultats de la recherche proprement dit, Google affiche en effet des annonces (parfois frauduleuses) en rapport avec les termes de la recherche. Ne cliquez jamais sur ces annonces si elles mentionnent votre établissement financier.
- Assurez-vous que la connexion est sécurisée (cadenas, nom de l'institut financier et nom de domaine corrects).

La vidéo aborde également la question du Remote Support. Le Remote Support ou assistance à distance est une technologie qui permet de bénéficier d'une aide extérieure sur un dispositif, sans la présence physique d'un technicien sur place. Les instituts bancaires ont eux aussi recours à ce type de service dans le cadre de leurs activités d'assistance clients. Veillez à respecter les règles suivantes lorsque vous utilisez cette technologie :

- N'appelez jamais les numéros de téléphone du service d'assistance ou du helpdesk indiqués dans les annonces Google.
- Établissez une connexion uniquement avec des personnes dignes de confiance. Soyez particulièrement méfiant, si vous n'êtes pas vous-même l'initiateur de la connexion.
- Utilisez une connexion sécurisée (cadenas, nom de l'institut financier et nom de domaine corrects).
- N'autorisez pas le contrôle total de votre système. La personne qui vous aide devrait se limiter à observer passivement ce que vous faites.
- Sachez que tout ce qui s'affiche à l'écran peut être vu et enregistré par votre interlocuteur.
- Ne naviguez pas sur des sites Internet n'ayant aucune pertinence avec l'objet de votre session, même si votre interlocuteur vous le demande.
- Une fois votre prise en charge terminée, assurez-vous que la connexion avec le centre de Remote Support est bien coupée pour empêcher tout accès futur à votre appareil.