Arnaques par téléphone : nos conseils de prévention

De plus en plus d'escrocs se font passer pour des conseillers travaillant au sein de votre banque ou d'organisme de notoriété pour vous soutirer des informations bancaires. Ils peuvent agir en vous envoyant des emails ou vous contacter par téléphone sur votre fixe ou mobile. Face à l'ampleur de ces arnaques, nous vous invitons à être vigilant.

Les différentes fraudes par téléphone

Le principe est généralement assez similaire et l'objectif le même : vous soutirer des informations qui peuvent être **revendues ou réutilisées** immédiatement **comme vos données personnelles ou bancaires.**

Phishing téléphonique :

Une personne vous appelle et se fait passer pour un employé de votre banque, site commerçant connu, ou tout autre enseigne de renom. Dans la conversation, l'usurpateur fera tout pour instaurer un climat de confiance pour vous soutirer des informations.

Ping calls :

Technique de spam vocal, cette arnaque vous incite à rappeler un numéro surtaxé. Généralement, vous constatez un appel en absence, ou vous avez un appel qui ne dure pas assez longtemps pour vous laisser décrocher à temps. Lorsque vous rappelez, vous avez gagné un bon d'achat ou un cadeau. On vous demandera vos informations personnelles ou même bancaires pour vous le faire parvenir. Attention, pour éviter toute méfiance, les numéros utilisés pour ces fraudes ne sont désormais plus des numéros comme des 0 800 mais des indicateurs tout à fait communs comme 01, 02, etc.

Vishing :

Cette fois, il s'agit d'un serveur vocal qui va, soit vous demander des actions à l'aide de votre clavier téléphonique, soit, si vous ne décrochez pas, vous laisser un message pour vous inciter à rappeler ou effectuer une action.

Smishing :

Un message à caractère urgent est envoyé par sms pour vous inciter à effectuer une action : soit rappeler un numéro, soit vous rendre sur une page internet.

Adopter les bons réflexes pour éviter la fraude

Quelque soit la technique à laquelle vous serez confronté, la méfiance reste la meilleure prévention.

- Ne jamais rappeler un numéro que vous ne connaissez pas ou sur lequel vous avez un doute,
- Rappeler plutôt le service client ou le numéro officiel de l'organisme vous ayant laissé un message ou contacté,
- Ne jamais donner vos coordonnées bancaires, numéros de carte et cryptogramme, identifiant de connexion, mot de passe, ou code reçu par sms,
- Contacter votre banque pour vérifier que vous n'êtes pas victime d'une fraude, même si vous n'avez pas fourni d'informations ou si vous avez un doute.

Que faire en cas de fraude téléphonique ?

Dans le cas où vous pensez être victime d'une arnaque, contactez au plus vite votre banque pour qu'elle vous accompagne dans les démarches à suivre.

Vous pouvez également signaler la fraude :

- Par SMS au **33 700** avec le texte « Spam vocal 01 XX XX XX XX » en précisant le numéro de téléphone suspect. Votre signalement sera transmis aux opérateurs.
  Recommandée par la DGCCRF, cette plateforme de signalement a été mise en place par les opérateurs de la fédération française des Télécoms. Vous pouvez y signaler une tentative d'arnaque par spam vocal (message vocal incitant à rappeler un numéro surtaxé).

- Par téléphone au 0 805 805 817 (cartouche vert service & appel gratuit) du lundi au vendredi de 9h à 18h30 pour signaler l'arnaque à la police nationale.