Arnaques numériques, téléphoniques : les réflexes à avoir

En cette période de crise sanitaire, des personnes peu scrupuleuses profitent de la situation pour tenter de vous escroquer.

1/ Arnaque au téléphone, réagir ou se laisser piéger, mais toujours agir !

Comment reconnaître une arnaque à l'appel téléphonique ?

Le numéro :
Si vous avez la possibilité de visualiser le numéro de téléphone, et que vous remarquez un indicatif étrange, un numéro venant de l'étranger, un numéro masqué, commencez à être méfiant.

La présentation :
Bien souvent la présentation des escrocs est rapide et peu compréhensible. Vous comprendrez mal le nom de votre interlocuteur. À l'inverse, certains escrocs n'hésitent pas à mentionner le nom d'un organisme officiel.
Dans le premier cas, la personne va jouer sur le degré d'urgence en allant immédiatement à l'essentiel : vous soutirer vos informations, dans le second cas, la personne utilise un argument d'autorité

Comment réagir face à ce type d'appel ?

Ne pas répondre

Ne répondez pas et laissez l'interlocuteur mettre un message sur votre messagerie. Dans la majorité des cas, s'il s'agit d'une arnaque, vous n'aurez aucun message. Dans le cas contraire, vous pourrez vérifier le message auprès de votre interlocuteur habituel de l'organisme qui prétend vous avoir contacté ou même votre conseil (votre expert-comptable par exemple en cas d'appel d'un prétendu service des impôts).
Simple mot d'ordre : si ce n'est pas important, il n'y a pas de message donc il n'y a pas besoin de rappeler. Et en cas de doute appeler votre interlocuteur habituel et non, le numéro qui vous a appelé !

09 avril 2020

Arnaques numériques, téléphoniques : les réflexes à avoir

Et si vous répondez, comment réagir ?

Questionner la personne. Prenez du recul et prenez le temps de faire répéter tous les éléments. Demandez son nom, le service dans lequel il ou elle travaille, l'adresse de la structure. Le fait de prendre le temps de questionner votre interlocuteur va :

1 être déstabilisé ;
2 vous permettre de prendre du recul ;
3 vous aider analyser la situation.

Ne donner aucune information :

Ne donner aucune information personnelle. Les structures officielles ont déjà ces éléments. Raccrocher rapidement et appeler vos conseillers habituels pour vérification.

Et si vous avez donné des informations ?

Si vous avez malheureusement donné des informations, appeler au plus vite vos conseillers et contacts (ex: votre conseiller bancaire s'il s'agit d'informations sur votre compte ou votre carte de paiement, votre expert-comptable s'il s'agit d'information sur des données concernant votre entreprise, le dirigeant de votre entreprise si l'interlocuteur se prétend être à son contact pour une affaire) qui vous accompagneront.
Si vous ne parvenez pas à les contacter par téléphone, faites-leur un mail. Pour les banques, il existe un numéro vert et le site internet ou votre application smartphone pour faire opposition et informer votre banque.

Simple mot d'ordre : si ce n'est pas important, il n'y a pas de message donc il n'y a pas besoin de rappeler. Et en cas de doute, appeler votre interlocuteur habituel et non le numéro qui vous a appelé !

09 avril 2020

Arnaques numériques, téléphoniques : les réflexes à avoir

2/ Arnaque par mail : ne pas agir par réflexe !

Comment reconnaître le plus souvent les arnaques par mail :

L'expéditeur, un doute ? Alors arnaque en vue :

Le nom ou le prénom de la personne vous semble familier ? Ils sont vraiment malins !
Mais ce n'est pas votre interlocuteur habituel alors suivez votre instinct, c'est une arnaque.

- des noms d'expéditeurs mal écris : ex : « A.M.A.Z.O.N » pour « Amazon ».
- un mail à rallonge ;
- une adresse avec un suffixe (.com ou .fr) différent de l'organisme.

servicemarketing@afigec.com 

servicemarketingafigec@gmail.com 

Le mail a une forme inhabituelle :
Mot d'ordre : faire attention à ce qui est inhabituel ! Votre premier sentiment est le bon : "bizarre ce mail"

- Le langage utilisé est trop familier ;
- Il y a des typographies inhabituelles (sigle de monnaies, langues étrangères, mots mal orthographiés, etc.)
- Les templates (organisation générale du mail) sont bien souvent grossiers et mal ajustés à la lecture ;
- Les logos sont souvent baveux et les certaines couleurs peuvent vous paraître « étranges ».
- Le titre de la pièce jointe n'est pas habituel ;
- Vous n'avez normalement jamais à ouvrir une pièce jointe alors que cette fois-ci votre interlocuteur vous le demande alors que vous en vous ne vous y attendiez pas ou le mail vous invite à cliquer sur un lien ;
- Le père noël n'existe pas : personne ne vous remboursera des millions et il n'y a pas d'erreur de la banque en votre faveur et ne passer pas par la case départ vers l'arnaque ;
- Vos comptes ne sont pas bloqués, il suffit d'appeler votre agence pour vous en assurer ;
- L'achat d'une cible par votre patron requiert plus qu'un mail pour approuver les virements de fonds demandés ;
- Votre interlocuteur qui a un pouvoir hiérarchique vous demande de déroger à une procédure habituelle ;
- Vous devez réinitialiser vos de passe alors que vous n'êtes pas allé sur le site concerné ;
- Mr XXX vous a laissé un message, veuillez cliquer ici pour le consulter ;

Arnaques numériques, téléphoniques : les réflexes à avoir

Comment réagir face à un mail douteux ?

- N'ouvrez pas le mail
- Ne cliquez pas sur le lien
- N'ouvrez pas la pièce jointe
- Contactez votre interlocuteur habituel pour confirmer qu'il a essayé de vous joindre (téléphone, mail, vidéo). Il comprendra votre besoin de sécurité, car lui aussi est soumis à ce genre d'arnaque !

Oui, mais j'ai quand même cliqué : que faire ?

L'ouverture d'un mail n'est en général pas génératrice d'une infection par un virus. Par contre, cliquer sur une pièce jointe ou en ligne ou même envoyer des informations doit être traitée en urgence :

- Débranchez votre ordinateur du réseau
- Contactez votre service informatique
- Confirmez avec votre interlocuteur habituel pour confirmer qu'il s'agissait d'un mail frauduleux
- Si besoin, contactez votre banque par tout moyen pour faire les oppositions de rigueur

Vous pourrez également contacter les services judiciaires pour informer de cette tentative d'arnaque qui pourrait avoir des préjudices pour vous et vos biens. Également, pensez à votre assureur qui peut avoir une procédure d'urgence et qui pourra aussi vous indemniser le cas échéant du cadre de votre couverture d'assurance.

Par ailleurs vous devrez également analyser votre situation en termes de RGPD et vos actions à mener.

Oui, mais ça y'est je viens de recevoir une demande de "rançon" pour débloquer mes matériels ?

Alors, contactez en urgence votre interlocuteur informatique, et les services judiciaires et votre assureur.

Mais heureusement vous aviez des sauvegardes dans le cloud que vous aviez déjà testées, n'est-ce pas ?

09 avril 2020

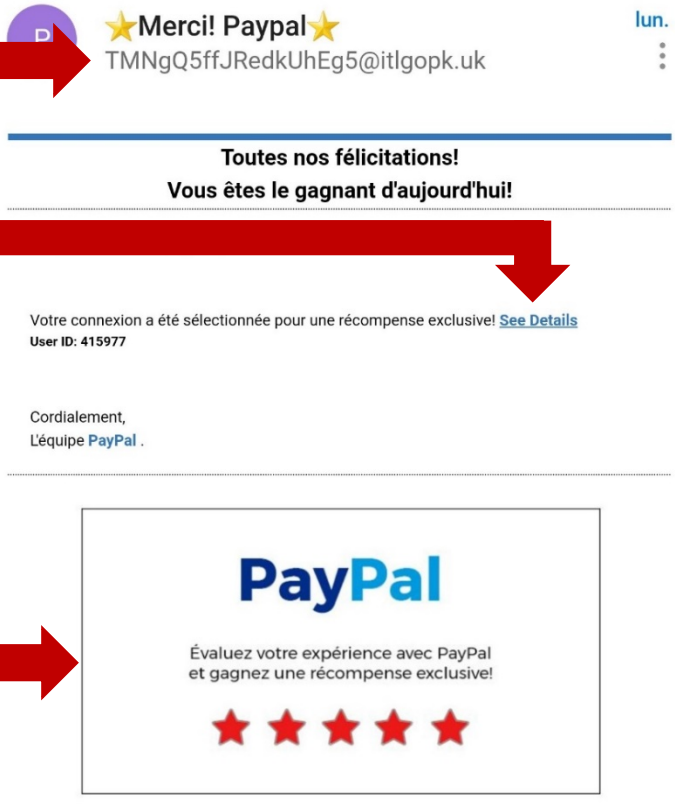
Arnaques numériques, téléphoniques : les réflexes à avoir

3/ Des exemples

Nom de l'expéditeur erroné

Message avec des icônes

Adresse mail très étrange



Bouton d'appel et en anglais

Logo baveux

09 avril 2020