TENTATIVES DE PHISHING : COMMENT LES REPÉRER ?

Ce mail vient-il vraiment de votre banque ? Il a un beau logo, il est bien écrit mais vous avez raison de vous méfier. Tous ne sont pas truffés de fautes d'orthographe et certains ont l'air plus vrais que vrais pour vous soutirer données et infos personnelles et accéder à vos comptes. Les tentatives d'escroquerie par phishing ou hameçonnage se multiplient. Comment les repérer ? Que faire si vous vous êtes fait piéger ?

VOICI 10 INFOS ET CONSEILS POUR REPÉRER LES MAILS FRAUDULEUX ET ÉVITER LES PIÈGES

1- Votre banque ne vous demandera **JAMAIS** de communiquer des informations sensibles par mail non sécurisé en dehors de votre banque en ligne, ni par téléphone. De même, votre Conseiller ne vous demandera **JAMAIS** le code personnel et confidentiel à 4 chiffres de votre carte bancaire, ni votre code d'accès à la banque en ligne, ni les codes de sécurité envoyés par SMS ou courriel pour valider des opérations dites sensibles, telles que l'enrôlement à Securipass du Crédit Agricole par exemple, ou la réalisation d'un virement.

2- **Ne cliquez JAMAIS sur un lien vous invitant à remplir un formulaire, dans un mail « classique » semblant venir de votre banque.** Il peut déclencher un logiciel malveillant qui récupèrera des données sur votre ordinateur.
Lorsque votre banque a besoin de vous contacter, elle vous envoie un courriel vous indiquant qu'un message est à lire dans votre espace personnel, en ligne ou sur l'application mobile. Ce message ne contient **JAMAIS** de lien à cliquer pour accéder à la banque en ligne : c'est une règle intangible que se sont donnée les banques, pour se différencier des « hackers ». C'est au client d'utiliser l'adresse qu'il connait, et qu'il a sans doute enregistrée comme favori dans son navigateur.

3- Faites preuve de bon sens : **tout ce qui commence par "confidentiel" ou "nous avons remarqué un problème sur votre compte" ou "votre compte a été restreint" ou " votre carte bancaire est suspendue", "veuillez valider ce remboursement", "concernant la Directive Européenne pour les services de paiements (DSP2), il est impératif de vous inscrire au service de confirmation mobile (SécuriPass)" etc.** est à 99% du phishing ! Mais il y a bien d'autres motifs possibles…les personnes malveillantes ont de l'imagination. Ces courriels sont la plupart du temps **anonymes** : on vous écrit « Cher client », « Madame, Monsieur », etc. il est assez rare que le courriel frauduleux mentionne votre nom.

4- **Qui vous envoie vraiment ce courriel ?** Vous lisez "De : Agence du Crédit Agricole "? Et lorsque vous passez la souris sur ce nom quelle adresse lisez-vous ? "capsule-123456-qqr@xxxx.com". Bref : rien à voir avec l'adresse électronique de votre conseiller du Crédit Agricole. Un escroc tente bien de se faire passer pour votre conseiller, ou pour une personne appartenant à votre banque.
Sachez cependant qu'un mail frauduleux peut afficher une adresse valide, même si c'est plutôt exceptionnel dans les attaques destinées au grand public : ce qui est expliqué aux points 2 et 3 est donc primordial.

01/2021 Extrait de conseils bancaires

5- Vous recevez un mail douteux après les heures d'ouverture de votre agence ? Vous hésitez à répondre ? Surtout **ne faites rien et attendez la réouverture de votre agence** pour vérifier la véracité du mail : **il y a très peu de situations qui nécessitent une réaction ou une réponse immédiate.**

6- **Vous vous êtes fait piéger** et avez communiqué des informations bancaires confidentielles ? Contactez votre agence bancaire au plus vite. Si celle-ci est fermée, **contactez le service d'assistance de votre carte bancaire** et faites opposition (mais seulement si vous avez transmis les caractéristiques complètes de celle-ci, c'est-à-dire son numéro, sa date d'expiration et le code à 3 chiffres au dos de celle-ci). Le numéro d'appel est indiqué au dos de votre carte bancaire. Et changez vos mots de passe d'accès au site de votre banque. **Surveillez vos relevés de compte bancaire** et assurez-vous qu'aucun montant n'a été débité de façon irrégulière. En cas d'anomalie, signalez le problème au plus vite à votre agence, en indiquant très clairement que vous n'êtes pas à l'origine de certains mouvements sur votre compte.

7- **Signalez le mail frauduleux** à votre banque et à la Police, sur ce site exclusivement pour que les escrocs soient bloqués au plus vite : https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

8- **Mettez à jour le système de protection de votre ordinateur** : antivirus, pare-feu, logiciel anti-espion... Utilisez des logiciels connus car il existe aussi de faux antivirus.

9- **Utilisez un filtre contre le "filoutage"** : la plupart des navigateurs internet proposent une fonction d'avertissement qui signale les sites suspects, quand vous êtes sur le point de vous y connecter. Allez dans les paramètres de votre navigateur pour activer ces fonctions.
Idem pour le filtre anti spam (ou pourriel) dans votre logiciel de messagerie, comme sur le site Web (Webmail) de votre fournisseur de messagerie.

10- Ces conseils sont valables pour les courriels de votre banque comme pour ceux **qui sembleraient venir d'un grand magasin, des impôts, de la CAF, des grandes plateformes Web...**

Enfin, attention sur les réseaux sociaux ! Ne publiez JAMAIS vos coordonnées bancaires (photos ou numéros de votre carte bancaire par exemple) ! Si vous devez payer quelque chose à partir des réseaux sociaux, vous devez obligatoirement être redirigé vers un site marchand **et vérifier qu'il est sécurisé.**

BON À SAVOIR

L'adresse d'un site internet sécurisé commence par https:// et doit comporter l'icône d'un petit cadenas fermé ou d'une clé.

Le phishing (ou « hameçonnage ») est une technique d'escroquerie par Internet de plus en plus utilisée par les escrocs pour voler des données personnelles : votre nom et votre adresse, vos coordonnées (téléphone, adresse postale, etc), votre date de naissance, votre numéro de compte bancaire, votre numéro de sécurité sociale, vos identifiants de connexion Internet à des sites bancaires ou à des sites marchands, vos codes de sécurité pour valider des opérations sur Internet... vos identifiants et mots de passe de messagerie, etc.

01/2021 Extrait de conseils bancaires