Un appel du service fraude de votre banque…

Attention ARNAQUE !

Jamais votre banque n'agira comme cela !

Raccrochez même si la personne insiste.

1°) Introduction

Les appels de faux service fraude des banques sont une technique courante utilisée par les escrocs pour obtenir des informations bancaires et personnelles. Cette présentation vise à vous aider à reconnaître et à vous protéger contre ces arnaques.

2°) Comment l'arnaque fonctionne

- *Appel téléphonique :* Un individu appelle en se faisant passer pour un représentant de votre banque. Souvent il prétend faire partie du « SERVICE FRAUDE ».

- *Tactique de peur :* Il vous informe d'une prétendue activité frauduleuse sur votre compte et vous demande des informations sensibles pour "vérifier" ou "sécuriser" votre compte. Le ton de la conversation peut devenir insistant, menaçant ou du style « *Hé bien faites ce que vous voulez, moi je suis là pour vous aider, si vous ne voulez pas de mon aide tant pis pour vous* ». Ne vous laissez pas convaincre !

- *Demande d'informations :* Il peut demander votre numéro de carte bancaire, votre code PIN, vos identifiants de compte en ligne, ou d'autres informations personnelles. Bien souvent il vous demande de lui communiquer le code que vous allez recevoir par sms/mails pour valider l'opération de blocage. Bien évidemment ce code ne servira pas à bloquer une transaction suspecte mais à vider vos comptes !

3°) Signes à surveiller

- *Urgence :* L'appelant insiste sur l'urgence de la situation pour vous inciter à agir rapidement sans réfléchir.

- *Informations sensibles :* Il demande des informations que votre banque ne vous demanderait jamais par téléphone.

- *Numéro inconnu :* L'appel provient d'un numéro inconnu ou non reconnu. Attention toutefois, le numéro affiché sur votre téléphone peut parfois correspondre à celui de votre banque.

4°) Que faire en cas d'appel suspect

- *Ne jamais donner d'informations personnelles :* Ne divulguez jamais d'informations bancaires ou personnelles par téléphone.

- *Vérifier l'appel :* Raccrochez et appelez directement votre banque en utilisant un numéro que vous connaissez ou qui est indiqué sur votre carte bancaire.

- *Signaler l'appel :* Informez votre banque et signalez l'incident aux autorités compétentes, comme par exemple Cybermalveillance.gouv.fr.

5°) Mesures de protection

- *Soyez vigilant : Méfiez-vous des appels inattendus qui demandent des informations sensibles.*

- *Mots de passe forts : Utilisez des mots de passe complexes et changez-les régulièrement.*

- *Surveillance des comptes : Vérifiez régulièrement vos relevés bancaires pour détecter toute activité suspecte.*

- *Authentification à deux facteurs : Activez l'authentification à deux facteurs pour sécuriser vos comptes en ligne.*

- *Demander de l'aide :* Vous n'êtes pas seul, vous trouverez de l'aide sur le site de cybermalveillance.gouv.fr.

6°) Conclusion

En restant vigilant et en suivant ces conseils, vous pouvez vous protéger contre les appels de faux service fraude des banques.

N'oubliez pas : votre banque ne vous demandera jamais vos informations sensibles par téléphone.

Si vous recevez un appel suspect, raccrochez et contactez directement votre banque par un numéro que vous connaissez.

Référent cybersécurité de la Gendarmerie de la Marne

Adjudant Yannick DUPONCHEL

Communication Référent Cybersécurité
Gendarmerie de la Marne
Châlons en Champagne

LA FRAUDE AU FAUX CONSEILLER BANCAIRE

Ce qui se passe en apparence...

Votre conseiller vous appelle par téléphone. Le numéro affiché semble bien être le sien. Il vous alerte sur des opérations qu'il dit "anormales".
Pour les annuler ou procéder à des vérifications, il vous demande d'agir directement sur votre téléphone ou de lui donner certaines informations.

Mais en réalité...

C'est un escroc qui vous fait réaliser des opérations. Au lieu d'annuler les opérations, vous en réalisez vous-même des nouvelles à son profit.
Si vous lui donnez des informations (cryptogramme, codes d'accès de banque à distance, ou code SMS de validation…) il pourra les réaliser lui-même.

Ce que vous devez faire...

- Raccrochez et contactez votre banque par un numéro de téléphone que vous connaissez et vérifiez l'information si vous avez un doute
- Ne donnez jamais suite à une telle demande. Jamais votre banque ne vous demandera : ni vos codes d'accès, ni votre cryptogramme visuel de carte, ni vos codes de validation.

- Ne communiquez à personne vos données bancaires et vos codes confidentiels.

- Ne validez jamais une opération par SMS si vous n'êtes pas certain de l'origine