



- ALERTE ARNAQUE INTERNET

ET SPOOFING -

Au cours de la semaine écoulée, la Gendarmerie du FINISTÈRE a enregistré plusieurs plaintes concernant des démarchages téléphoniques abusifs par de « faux conseillers bancaires » - dit *SPOOFING*.

LE SPOOFING ... C'EST QUOI ?

- ① --> « Bonjour, je suis M. Dupont MENTEUR, votre conseiller bancaire à la Banque BANCALE. Nous avons détecté des activités suspectes sur votre compte ... et je vais vous aider à résoudre ce problème. »
- ② --> Il s'agit d'une technique frauduleuse : le spoofing.
- ③ --> Grâce à un logiciel et / ou plateforme, l'escroc fait afficher sur votre téléphone portable le numéro réel de votre banque et / ou celui des services de police ou de gendarmerie – dans le but de gagner votre confiance. Ensuite, il déroule son scénario.

NOTA : Certains délinquants se présentent également par téléphone comme policier ou gendarme ... en prétextant agir dans le cadre d'une enquête judiciaire.

- RAPPEL --> 4 « règles d'or » de prudence -

- Ne cliquez **jamais** sur le lien, ni les pièces jointes transmis par SMS ou courriel.
- Ne rappelez **jamais** directement le N° utilisé par ce correspondant indélicat.
- Votre conseiller bancaire, les policiers ou les gendarmes ne vous demanderont **jamais** par téléphone vos coordonnées bancaires, vos codes d'accès, etc.
- Au moindre doute, contactez vous-même votre conseiller habituel et signaler la pratique sur **17CYBER**¹

En cas de doute =

1 réflexe --> faites le 17

Merci pour votre aide et pour votre vigilance !



¹ <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/page/17cyber-mon-assistance-en-ligne>

Spoofting ou arnaque au faux conseiller bancaire

“

Bonjour, je suis M. DUPONT Menteur, votre conseiller bancaire à la Banque BANCALE. Nous avons détecté des activités suspectes sur votre compte et nous avons besoin de vérifier certaines informations pour votre sécurité.

”

Faux conseiller bancaire

La victime reçoit un appel d'un pseudo conseiller bancaire. Elle doit **fournir ses identifiants / coordonnées bancaires rapidement** pour annuler des opérations frauduleuses sur son compte bancaire.

Comment le reconnaître ?

Le ton est urgent et alarmant !

Globalement, il s'agit :

- D'un appel **prétextant des opérations frauduleuses** dont le client n'a pas connaissance.
- D'une **demande de coordonnées bancaires** en ligne ou par téléphone sans que le client en soit à l'origine.

#Prévenir

Le faux coursier

En se faisant passer pour un conseiller bancaire, le malfaiteur propose de venir **recupérer votre carte bancaire " bloquée " directement à votre domicile.**

Restez vigilant

- Les escrocs peuvent utiliser **le numéro de téléphone de votre banque et/ou usurper l'identité de votre conseiller bancaire.**
- Ils rassurent leurs victimes en précisant votre nom, votre adresse et le nom de votre conseiller bancaire.

Comment éviter les arnaques au faux conseiller bancaire ?



Vous recevez un message /mail douteux.

NE CLIQUEZ PAS SUR LE LIEN, NI SUR LES PIÈCES JOINTES



AU MOINDRE DOUTE, CONTACTEZ VOUS-MÊME L'ORGANISME EN QUESTION.



NE RAPPELEZ PAS LE CORRESPONDANT DIRECTEMENT.



JAMAIS VOTRE CONSEILLER BANCAIRE NE VOUS DEMANDERA VOS COORDONNÉES BANCAIRES.

