BANQUE POSTALE - LA TENTATIVE DE FISHING - HAMEÇONNAGE

Categories: Actualités ADC FRANCE, Banques & organismes de crédit, Les conseils
Tags: Conseils, Enquête

Le fishing contre la Banque postale est considérable. Un de nos adhérents reçoit parfois deux mails par jour ! Nous avons voulu en savoir plus. Nous avons pris un mail reçu et regardé la situation. Le mail envoyé part du Japon !!! En bas de cet article, nous vous communiquons le lien caché derrière " ACTIVEZ LE SERVICE" pour chaque mail frauduleux identifié avec le nom de la banque.

Le mail

Nous publions le contenu du courriel :

"Notification@labanquepostale.fr

Chèr(e) client(e),

Vous avez choisi de gérer vos comptes en ligne depuis le site labanquepostale.fr ou l'application La Banque Postale business, mais vous n'avez pas encore ***reconfirmé*** *votre numéro de mobile dans votre profil.*

ATTENTION : à ***partir du 15 novembre 2022****, afin de renforcer votre sécurité et conformément à la*

seconde directive européenne sur les services de paiement[2], ***votre identifiant et votre code secret de connexion ne suffiront plus*** *pour accéder à votre Espace Client.*

Tous les 90 jours calendaires, une authentification forte sera nécessaire. Pour cela, vous devez réactiver votre numéro de mobile à l'aide du code unique reçu par ***courrier*** *ou par* ***sms****. À défaut, l'accès à votre Espace Client sera bloqué !*

Pour continuer à rester connecté à vos comptes, merci de reconfirmer votre numéro mobile et de reactivez votre service :

ACTIVEZ VOTRE SERVICE

Merci de votre confiance,
Cordialement."

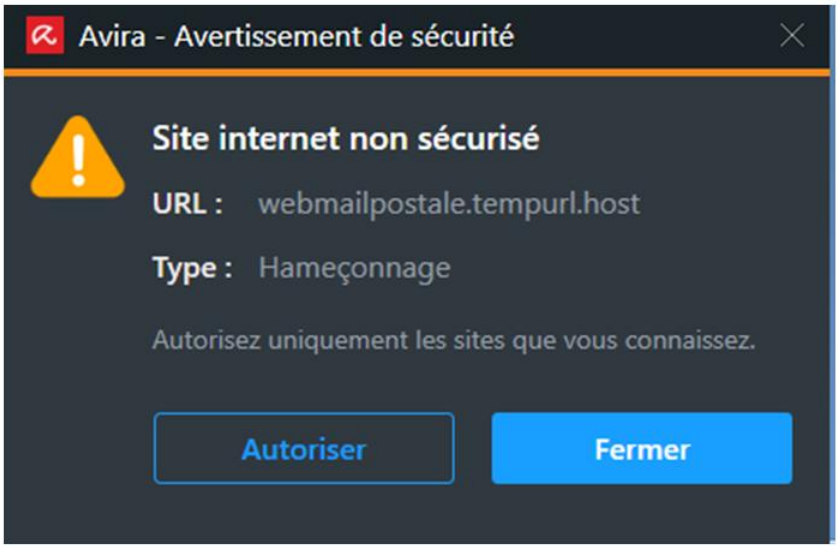
NDLR : Le gras a été mis par les arnaqueurs.

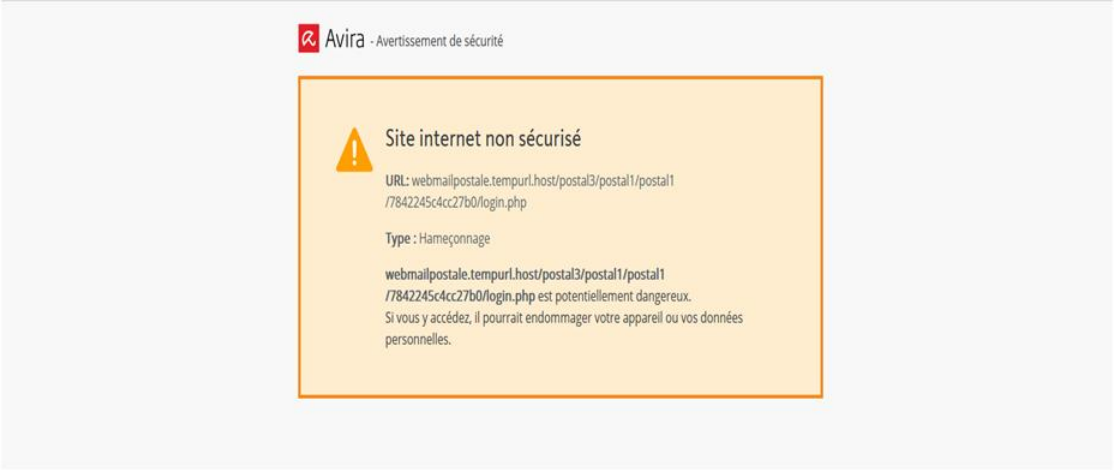
L'adresse apparente pour la réponse est **La Banque Postale <Notification@labanquepostale.fr>**

Tout semble normal...

Nos recherches

Pour activer le service, il faut cliquez sur le lien. Notre anti-virus nous a bloqué quand nous avons entré son adresse dans la barre de navigation :





Nous avons regardé qui nous envoyait réellement ce mail frauduleux.

Avec le clic droit de la souris, vous demandez le code source. Il s'agit de la vraie écriture en html utilisée.

Cela donne comme résultat :

compte1

X-UIDL : UID258-1665510962

Statut X-Mozilla : 0001

X-Mozilla-Statut2 : 00000000

Clés X-Mozilla :

Return path / Chemin de retour : <anonymous@s205.xrea.com>

X-Original-To :

Livré à :

Received / Reçu : depuis s205.xrea.com (s205.xrea.com)

NDLR : Le gras et la couleur ont été ajoutés par nos soins.

Cela signifie qu'il est utilisé le site xrea pour l'envoi du mail et pour répondre.

Pour voir qui vous envoie ce mail, vous regardez en haut de la page en code source. Vous avez le nom avec chemin de retour pour votre réponse et return path / reçu pour le nom du site qui vous l'a envoyé. Ce ne sont pas forcément les mêmes.

Le site xrea.com est en fait une société de prestations de services internet japonaise. Elle n'est pas à l'origine ni complice de cette arnaque.

On est loin de la banque postale...

Autres liens

L'envoi de ces messages frauduleux est incessant. Nous publierons dans cette partie de l'article le lien réel qui se cache derrière "ACTIVEZ VOTRE SERVICE" ou toute autre formule.

Banque Postale

- https://webmailmessageriepostale.tempurl.host/2022/messagerie/
- https://webpostalecontact-secur22.tempurl.host/GFDUYJQGKFHLKJFS/7842245c4cc27b0/login.php (2 fois)
- https://potsalebanque-entreprises22.tempurl.host//YURFSGGJYJSGHGFC/7842245c4cc27b0/login.php
- https://scalemyads.in/mac/dau3/isaacnetero.php (**réactivation du contrat**)
- https://webmailpostale.tempurl.host/postal3/postal1/postal1/7842245c4cc27b0/login.php

Le fishing continue comme le montre l'alerte publiée ci-dessous

https://www.signal-arnaques.com/scam/view/703249

Banque Populaire

https://cjoint.com/doc/22_11/LKjpz6SHKMa_miseajour.html

Banque axa

https://urly.it/c/102 - lien raccourci supprimé.

https://tinyurl.com/2eahzjxu - lien raccourci du site
https://drogariamarcelino.com/wow/lokija/index.html

Crédit Agricole

https://sites.google.com/view/ssffgfytygh/accueil

Carrefour Banque

https://urly.it/c/11g (espace client carrefour)

Il s'agit d'un lien raccourci qui ne s'ouvre pas.

Surtout NE RÉPONDEZ A AUCUN MAIL REÇU ou SMS quelque soit l'origine !