Le Consom'Acteur

UFC-Que Choisir Sète Bassin de Thau

n°10 - 4°trimestre 2023

Sommaire

LE MOT DU PRÉSIDENT

Chères adhérentes, chers adhérents,

Que cette nouvelle année 2024 vous apporte joie, bonheur et santé ainsi qu'à vos proches.
Je vous adresse tous mes meilleurs vœux, et toute l'équipe de bénévoles se joint à moi pour vous souhaiter le meilleur pour 2024.

L'évolution numérique progresse de plus en plus rapidement et facilite l'action des fraudeurs ainsi que tous autres arnaqueurs dont l'imagination et les méthodes nous surprennent de plus en plus.
Nous ne cesserons jamais de vous mettre en garde contre de faux sites commerciaux ou gouvernementaux.
Ceci vaut également pour les sollicitations téléphoniques .
Votre vigilance doit être permanente, n'hésitez pas à nous contacter avant un achat important par internet sur un site que vous ne connaissez pas.
La ténacité et la persévérance de nos bénévoles permettent dans la grande majorité des cas de régler les litiges à l'amiable.

Je vous remercie pour la confiance que vous faites à notre Association de défense des consommateurs, votre adhésion est précieuse pour poursuivre nos efforts pour faire valoir vos droits.

Nous vous invitons d'ores et déjà à assister à notre assemblée générale qui aura lieu à Sète, salle Tabouriech le 14 mars 2024 à 14 h 30.

APPELS TELEPHONIQUES FRAUDULEUX

Qu'est ce que le faux appel téléphonique?

Le faux appel téléphonique (vishing) est une technique d'escroquerie courante parmi les cybermenaces.

Le vishing, ou technique d'hameçonnage par téléphone, est une pratique criminelle d'ingénierie sociale qui consiste à communiquer avec des gens par téléphone dans le but de les frauder.
Cette fraude utilise habituellement la voix sur IP à cause des possibilités de cette technologie et son coût très bas.

L'appel téléphonique est passé directement par le fraudeur qui utilise une fausse identité.

Exemples:

- La personne se fait passer pour un conseiller bancaire ou un technicien des impôts, du Services des Fraudes ou encore de la maintenance informatique pour arriver à ses fins.
  Elle vous contacte dans le but d'obtenir vos codes de carte bancaire et de banque à distance.

- Vous naviguez sur internet, un message vous avertit que votre PC est bloqué. Il vous invite à appeler un numéro. Ce numéro est celui d'un faux support technique qui va vous soutirer de l'argent et vos coordonnées bancaires en prétendant réparer votre équipement.

- A la suite d'une annonce que vous publiez sur un site de vente en ligne, un faux acheteur vous contacte afin de récupérer des informations lui permettant d'initier une opération frauduleuse.

Les cybercriminels usurpent également l'identité d'organismes connus comme le Trésor Public, l' Assurance Maladie, les Opérateurs de mobiles ou de Services de Streaming, les services de livraisons, la CAF, etc...,pour vous tromper plus facilement.

Exemple:

- L'interlocuteur qui vous appelle sous une fausse identité, vous signale que le dernier paiement du mobile a été rejeté et vous demande la confirmation de votre code de carte bancaire ou code de banque à distance (BAD) dans le but de réactiver votre forfait et d'effectuer des achats frauduleux ou des virements à vos dépends.

Notez que les cybercriminels savent afficher le numéro de l'appelant usurpé. Le numéro et la localisation de l'appelant ne sont pas gage de sécurité, ils peuvent disposer d'informations personnelles vous concernant, pour vous rassurer.
Ils sont très forts!

CONSÉQUENCES POUR LES VICTIMES

Les conséquences sont multiples, le plus souvent financières:

- Bloquer l'accès à vos comptes (banque à distance) ainsi que vos moyens de paiement,

- Voler vos données (personnelles ou bancaires, usurpation de votre identité),

- Débit frauduleux sur vos comptes.

COMMENT SE PROTÉGER?

Les faux appels téléphoniques se basent sur l'usurpation d'identité pour vous mettre en confiance, la voix est chaleureuse et crée un sentiment de proximité contrairement aux messages reçus par mail ou SMS. C'est pour cela qu'il faut se méfier et toujours garder son sans-froid.

- Ne cédez pas au caractère urgent et pressant de la demande, qui doit au contraire vous interpeller,
- Ne validez pas une action dont vous n'avez pas été l'initiateur,
- Refusez toute demande de prise de contrôle à distance de votre ordinateur, tablette ou téléphone.
- Si un appel provenant de votre banque vous parait suspect, raccrochez et contactez votre conseiller en utilisant ses coordonnées habituelles ou allez le voir à la banque pour avoir confirmation de la demande.
- Vous pouvez contacter notre association,
- Conservez les preuves de la fraude en vue d'un dépôt de plainte auprès de la police, la gendarmerie ou sur les sites du service-public.fr.

Les faux appels téléphoniques et la cybercriminalité continueront à prospérer tant que les fraudeurs arriveront à leurs fins. Prendre le temps d'identifier les tentatives d'hameçonnages et surtout réussir à les déjouer est la meilleure façon de vous protéger.

QUELQUES PRINCIPES LIES AUX OPERATIONS BANCAIRES COURANTES.

1. Consultez très régulièrement le détail des opérations qui passent sur votre compte.
2. Si vous constatez un prélèvement inhabituel pour lequel vous n'avez pas donné d'autorisation, demandez le rejet de cette opération à votre banque. Vous disposez de 13 mois pour le faire.
3. S'il s'agit d'un prélèvement que vous avez autorisé pour lequel vous n'êtes plus d'accord, vous avez 8 semaines pour demander le rejet. Si vous demandez une révocation du mandat de prélèvement à votre banque l'organisme ne pourra plus émettre d'opérations sur votre compte. Cette démarche ne vous dispensera cependant pas de régler le différent avec l'organisme en cause.
4. Vous avez un an et 8 jours pour remettre un chèque en banque. Au-delà il n'est plus encaissable.
   Vous remettez un chèque sur votre compte: il peut être rejeté jusqu'à 8 jours après remise pour défaut de provision, ou pendant des délais plus longs, qui peuvent aller jusqu'à plusieurs mois en cas de faux chèque, chèque falsifié ou volé ou chèque tiré sur une banque étrangère.

Dans tous les cas soyez très méfiant si vous recevez un chèque d'une personne que vous ne connaissez pas ou peu, ou si on vous remet un chèque d'un montant supérieur à ce que l'on vous doit en vous demandant de renvoyer la différence sous forme de virement ou de mandat PCF, cette escroquerie se développe de plus en plus et la plupart du temps le chèque revient sans provision...

5. Le virement est une forme de paiement qui devient habituel. Le virement, une fois exécuté, ne peut plus être annulé. Si vous avez un virement à faire pour un fournisseur, sauf s'il vous a remis un RIB en main propre, n'hésitez pas à lui téléphoner sur son numéro habituel pour confirmation de sa domiciliation.

Vous avez un doute ou une question, n'hésitez pas à nous contacter. Nos conseillers sont à votre disposition. Ce sont des spécialistes et vous pouvez avoir confiance.

ALERTE QUISHING

L'association Ufc-Que Choisir alerte sur le «quishing», cette nouvelle arnaque qui est inspirée de l'hameçonnage, ou phishing. L'objectif est le même: il s'agit de vous faire cliquer sur un lien frauduleux et de récupérer vos données personnelles, comme les mots de passe ou les coordonnées bancaires.
Mais cette fois-ci, le fameux lien est caché derrière un QR code. D'où son nom de «quishing», contraction de QR code et de phishing.

Quelques exemples de ce à quoi vous pouvez être confrontés :

Arnaque parking de supermarché

Les escros accostent leurs victimes à la sortie de grandes surfaces (par exemple Leclerc, Carrefour, Intermarché…) en se faisant passer pour un membre du personnel. Ils expliquent ensuite à la cliente ou au client piégé qu'il ou elle a trop payé lors de ses courses. Résultat, pour se faire rembourser, les victimes doivent donner leur carte bancaire avec leur code secret. Ensuite, le voleur ou la voleuse se dirige vers un distributeur automatique pour retirer le maximum d'argent.

Arnaque à la fiente de pigeon

Le pickpocket va asperger sa cible d'un produit ressemblant en tout point à de la fiente de pigeon puis attendre que la personne se rende compte quelle a été la cible du volatile. Quand la victime commence à se tortiller pour tenter de se nettoyer, un bon samaritain lui propose son aide.
C'est là que disparaissent généralement portefeuilles, smartphones ou bijoux.

Arnaque à la facture Engie

Une arnaque par e-mail circule, prétendant que vous avez une facture impayée auprès d'Engie. Des individus malveillants utilisent alors des e-mails trompeurs pour inciter les destinataires à appeler un numéro de téléphone spécifique (09 77 40 06 38) et à effectuer un virement bancaire vers un IBAN mentionné dans le message. Soyez très prudent face à de telles communications, car elles pourraient être des tentatives d'escroquerie visant à soutirer de l'argent ou des information personnelles . Il est essentiel de ne pas répondre à de telles sollicitations et de signaler immédiatement toute activité suspecte aux autorités compétentes.

Dossiers gagnés par votre AL

Arnaque au faux chèque

M. X avait une créance de 1500 € pour la réservation d'une location saisonnière. Il fournit son iban en vue d'un virement. Le futur locataire envoie directement à la banque de M. X un chèque de banque d'un montant nettement supérieur. Il contacte M. X en indiquant qu'il s'agit d'une erreur de montant et lui demande de lui faire un virement du trop perçu. M. X s'exécute. Quelques jours après le chèque est rejeté au motif faux chèque. Le compte de M. X est débité du montant du chèque. L'AL obtient le remboursement du montant du chèque en arguant du fait que la banque n'a pas procédé aux contrôles qui s'imposent en matière de chèque de banque, en particulier la présence de filigranes.

Remise de liquidités non créditée

Mme B a effectué une remise d'espèces à l'automate de sa banque, l'automate a buggé, sa carte et les billets ont été avalés, elle n'a pas eu son reçu. Mme B a immédiatement porté réclamation.
24 jours après la situation n'était toujours pas régularisée, elle l'a été après la mise en demeure effectuée par l'AL.

Achats frauduleux sur internet

M. L est victime de plusieurs achats frauduleux sur internet avec sa carte bancaire. Ces achats sont d'un montant unitaire inférieur à 30 euros. La banque refusait le remboursement. L'AL est intervenue pour rappeler à la banque qu'il n'y pas d'obligation d'authentification forte pour un tel montant, mais en revanche la banque a l'obligation de rembourser si de telles opérations sont contestées. Ce qui a été fait.

Faux conseiller bancaire

Mme V a été contactée par un faux conseiller bancaire. C'est le n° du service fraude de la banque qui s'affichait. Il lui indique qu'un piratage est en cours sur son compte, il paraît très professionnel.
Il met la pression auprès de Mme V et lui fait effectuer diverses manœuvres sur son application de banque en ligne pour annuler les opérations frauduleuses. Mme V, mise en confiance, s'exécute, mais au lieu de lui faire annuler les opérations il les lui a fait valider.
La banque a refusé de rembourser au motif qu'elle avait elle même utilisé ses codes pour valider ces opérations. L'AL a rappelé au Médiateur que plusieurs jurisprudences ont condamné les banques lorsque c'était le n° de téléphone de la banque qui était utilisé. Mme V a été remboursée de la totalité des achats frauduleux.

Prélèvement non autorisé

Free a d'autorité prélevé sur le compte de M. T qui n'a pas transmis ses références bancaires à cet organisme. Free interrogé a indiqué qu'il s'agissait d'un accord avec la banque. Ce prélèvement a généré des frais. L'AL a dû intervenir pour obtenir le remboursement du prélèvement et des frais de la part de la banque.

NOS RENDEZ-VOUS

Votre association locale organise très régulièrement, en partenariat avec la Gendarmerie et les Mairies, des réunions d'information et de prévention. N'hésitez pas à consulter notre site internet et les réseaux sociaux pour en être informé.

Site internet : https://sete.ufcquechoisir.fr
Facebook : UFC Que choisir Sète Bassin de Thau
Instagram : @ufcquechoisirsetebassindethau

Taux d'intérêt légal

1° semestre 2024 professionnel: 5,07%
particulier: 8,01%

Dernier indice IRL connu

Trimestres	Parution au JO	Indices	Variation
4°trimestre2023	*16/01/24*	142,06	3,50%
3°trimestre2023	*13/10/23*	141,03	3,49%
2°Trimestre2023	*13/07/23*	140,59	3,50%
1°Trimestre2023	*14/04/23*	138,61	3,49%
4°Trimestre2022	*13/01/23*	137,26	3,50%
3°Trimestre2022	*14/10/22*	136,27	3,50%

UNION FEDERALE DES CONSOMMATEURS QUE CHOISIR
ASSOCIATION DE SETE BASSIN DE THAU
Tel:04 67 53 10 05 et 04 30 41 53 30
mail: contact@sete.ufcquechoisir.fr
site: http://sete.ufcquechoisir.f

NOS PERMANENCES

- **Sète:** C.C. Château Vert Bd Chevalier de Clerville
  Lundi de 14h à 17h
  Mardi, Mercredi, Jeudi, Vendredi de 9h à 12h

- **Agde**: Maison de la Justice et du Droit 04.67.35.83.60
- Espace Mirabel sur rendez vous
- le lundi de 14h à 16h30
- le mercredi de 14h à 16h30

- **Balaruc les bains**: Espace Louise Michel CCAS rue des écoles
  le mardi de 14 h à 16 h 30

- **Frontignan**: France Services 5 rue député Lucien Salette
  le 1° et 3° lundi de chaque mois de 9h30 à 11h30

- **Marseillan**: Rue de l'abbé Grégoire,sous les halles(locaux du restaurant des anciens)
  le 1° et 3° mardi de chaque mois de 9h à11h30

Mèze Locaux Cavalerie 2, rue de l'horloge n°2 près du porche
le 2°,3°et 4°Mercredi de chaque mois de9h à12h