Les données de votre carte de crédit ou vos coordonnées bancaires ont-elles été volées ?

Chaque jour, un nombre croissant de consommateurs profite des possibilités d'achats en ligne. Mais les acheteurs doivent rester prudents, car les escrocs en ligne cherchent toujours le moyen de leur voler leurs coordonnées bancaires ou les données de leur carte de crédit !

Ils utilisent des sites web frauduleux, se présentent comme des vendeurs sur les sites d'enchères et peuvent également envoyer des courriels frauduleux (hameçonnage) prétendant qu'ils font partie de sites de paiement ou de vente bien connus.

Que faire ?

Si la sécurité de votre compte bancaire a été compromise ou si vous remarquez une activité inhabituelle sur votre compte de carte de crédit, voici quelques mesures à prendre :

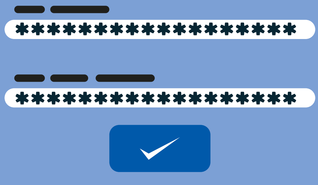
1. Contactez immédiatement votre établissement financier et faites bloquer votre carte de crédit/carte bancaire. Vous pourriez ainsi vous faire rembourser et empêcher un nouveau détournement.

2. Changez vos mots de passe. Il se pourrait que le fraudeur détienne votre mot de passe. Remplacez-le donc par un mot de passe robuste comportant au moins 15 caractères, y compris des majuscules et des minuscules, des minuscules, des chiffres et des caractères spéciaux.

Une phrase de passe peut être plus facile à mémoriser. Il peut s'agir, par exemple, d'une phrase qui comprend des mots peu courants ou provenant de langues différentes.

Vous devriez également modifier les données de connexion pour tout autre compte utilisant un nom d'utilisateur et/ou un mot de passe identique ou proche.

Utilisez un mot de passe unique pour chaque compte.



3. Mettez à jour votre logiciel antivirus afin de contrer les nouveaux virus et de protéger votre appareil.

63%

4. Signalez la fraude. Vos informations peuvent aider à attraper le fraudeur et à prévenir de nouveaux incidents.

Pour savoir où trouver conseil et à qui signaler une fraude dans votre pays, consultez le site https://cybersecuritymonth.eu/cyber-first-aid

5. Veillez à conserver toute preuve de la fraude subie, par exemple : courriels, factures, reçus, copie de l'annonce, etc.

6. Partagez votre expérience avec votre famille et vos amis pour les aider à se protéger.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick